Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Degree in Mathematics

Bachelor's Degree Thesis

Arcs, linear sets and hermitian curves in the finite projective plane.

Jordi Jofre Senciales

Supervised by Simeon Ball

September, 2018

Thanks to Simeon Ball.

Abstract

The main object of the study of this thesis are arcs in $PG(2, q^2)$. An arc in $PG(2, q^2)$ is set of points with the property that every line intersects with the arc in at most 2 points. One can prove that an arc in $PG(2, q^2)$ has at most $q + 2$ points and one would like to find arcs which contain a lot of points. An arc is equivalent to a maximum distance separable code. The larger the arc, the longer the code and the greater error-correcting properties the arc will have. In Section 3 we study arcs of size $q + 1$ that are the set of zeros of a quadratic form. In Section 4 we will study an arc constructed as the intersection of two hermitian curves. This arc is of size $q - \sqrt{q} + 1$ and is not contained in a conic. In the last section we study the intersection between a linear set and a hermitian curve. Firstly we calculate some examples in GAP. Then we prove some results about hermitian curves that will help us to interpret the computational results. We will prove that the intersection between a linear set over scattered space and non-degenerate hermitian curve is an arc.

Keywords

Arcs, MDS codes, Hermitian curves, Linear sets, Scattered subspaces

Contents

1. Introduction to projective geometry

1.1 Projective Space

We start with a short introduction to projective geometry.

Let $\mathbb{P}$ be a set. Let $\mathbb{K}$ be a field. Let E be a vector space over $\mathbb{K}$. A projective space is the triplet $(\mathbb{P}, E, \pi)$ where $\pi : E - \{0\} \longrightarrow \mathbb{P}$ such that:

- π is surjective.
- $\pi(u) = \pi(v) \Longleftrightarrow \exists \lambda \in \mathbb{K}^*$ such that $u = \lambda v$.

The dimension of $\mathbb{P}$ is $rank(E) - 1$. We will denote the elements of $\mathbb{P}$ as $p = \pi(u) = [u] = [u]_\pi$. In this thesis we will use dimension for the dimension of a projective space and rank for the dimension of vector space.

Definition 1.1. Let E a vector space over $\mathbb{K}$ of dimension $n+1$. Let $P(E) = \{$subspaces of E of dimension $1\}$. $\pi : E - \{0\} \longrightarrow P(E)$ defined by $\pi(u) =< u >$. Then $(P(E), E, \pi)$ is a projective space of dimension n.

1.2 Projective subspaces

Definition 1.2. A projective subspace is a subset L of $\mathbb{P}$ such that $L = \pi(F - \{0\})$ where F is a vector subspace of E. We will denote $L = [F]$.

Lemma 1.3. *Let $L = [F]$ projective subspace of $\mathbb{P}$. Then we have:*

1. $\pi^{-1}(L) = F - \{0\}$.
2. $F = \pi^{-1}(L) \cup \{0\}$.
3. *Moreover, if we have $p \in L$ and $u \in E$ such that $p = \pi(u)$ then $u \in F$.*

Proof. We know that $L = \pi(F - \{0\})$, taking π^{-1} in each part we have $\pi^{-1}(L) = \pi^{-1}(\pi(F - \{0\})) = F - \{0\}$. To prove the last equality, it's clear that $F - \{0\} \subset \pi^{-1}(\pi(F - \{0\}))$. To prove the other inclusion:

$$v \in \pi^{-1}(\pi(F - \{0\})) \Rightarrow \pi(v) \in \pi(F - \{0\}) \Rightarrow$$

$$\exists u \in F - \{0\} \; s.t. \; \pi(u) = \pi(v) \Rightarrow u = \lambda v, \lambda \in \mathbb{K}^* \Rightarrow v \in F - \{0\}$$

2 is an immediate consequence of 1.
For 3 we have $p \in L$ and $u \in E$ such that $p = \pi(u)$ using this $\pi(u) \in L \Rightarrow u \in \pi^{-1}(L) = F - \{0\} \Rightarrow u \in F$. □

Corollary 1.4. *Let $L_1 = [F_1]$ and $L_2 = [F_2]$ be projectives subspaces then we have:*

1. $L_1 \subset L_2 \Leftrightarrow F_1 \subset F_2$
2. $L_1 \subset L_2 \Rightarrow dim(L_1) \leq dim(L_2)$

3. $L_1 \subset L_2$ *and* $dim(L_1) \leq dim(L_2)$ *then* $L_1 = L_2$

We can define the following operations on projective subspaces $L_1 = [F_1]$ and $[L_2] = [F_2]$, the intersection and the sum:

- Sum: The sum of two projective subspaces is the smallest projective subspace which contain them. We can check easily the formula $L_1 + L_2 = [F_1 + F_2]$.
- Intersection: The intersection of two projective subspaces is a projective subspace. We can prove it by the following equality: $L_1 \cup L_2 = [F_1 \cup F_2]$.

Definition 1.5. Let $A = \{P_i\}_{i \in I}$ be a family of points of a projective plane P where $P_i = [v_i]$. We will say the points of A are independent if $\{v_i\}_{i \in I}$ are linearly independent.

1.3 Projective references

Let E be a vector space over the field $\mathbb{K}$. Let $\mathbb{P} = (\mathbb{P}, E, \pi)$ a projective space of dimension n. We want to find a bijection with good characteristics between $\mathbb{P}$ and $P(\mathbb{K}^{n+1})$. For this reason we introduce projective references.

Definition 1.6. Let $R = \{p_0, ..., p_n; U\}$ be a family of points of $\mathbb{P}$ where any subfamily of size $n+1$ is independent. We will say that R is a projective reference.

Definition 1.7. Let $e_0, ..., e_n$ be a basis of E. I will say this basis is adapted to the projective reference R if we have the following relation: $p_i = [e_i]$ and $U = [e_0 + ... + e_n]$.

There always exists an adapted basis over R. We can assume that $p_i = [v_i]$ and $\{v_i\}_i$ form a basis over E because $\{p_0, ..., p_n\}$ is a independent family. If we have that $U = [u]$ we can write u as a linear combination of $\{v_i\}$: $u = \lambda_0 v_0 + ... + \lambda_n v_n$. If we take $e_i = \lambda_i v_i$ then $\{e_i\}$ is an adapted basis over R. Reciprocally, if we take $\{e_0, ..., e_n\}$ a basis of E then it is adapted to the reference $R = \{[e_0], ..., [e_n]; [e_0 + ... + e_n]\}$.

Definition 1.8. Let R be a projective reference. Let B be an adapted basis over R. Let $p = [v] \in \mathbb{P}$. If the coordinates of v with respect to the basis B are $(v_0, ..., v_n)$, then we will say that the coordinates of p with respect to the reference R is the object $[(v_0, ..., v_n)] \in P(\mathbb{K}^{n+1})$.

1.4 Equations in projective spaces

Let $\mathbb{P} = (\mathbb{P}, E, \pi)$ be a projective space. Let R be a projective reference and $\{e_0, ..., e_n\}$ be an adapted basis. Let V_e denote the coordinates in this basis of a vector v.

Let L a projective subspace of $\mathbb{P}$ where $L = [v_0, ..., v_d]$. Let $p = [x] \in \mathbb{P}$ then we have $p \in L \Leftrightarrow x \in < v_0, ..., v_n > \Leftrightarrow X_e \in < V_{0,e}, ..., V_{n,e} >$. The last expression helps us to find an equation of the projective subspace in the reference R.

Now we are going to introduce the conics. Let $S_2(E) = \{\text{bilinear forms of E}\}$. We will define quadrics using the objects of $P(S_2(E))$ in the following way. (I will refer to these objects as conics when $\mathbb{P}$ have dimension 2). We define $Q = [\phi]$, a quadric, as follows. The set of points of Q is $\{p \in \mathbb{P} | p = [x], \phi(x, x) = 0\}$. Note that the condition $p \in Q$ does not depend on the representative of p.

Let us deduce the equation of a quadric. Let $Q = [\phi]$ be a quadric and $M = M_e(\phi)$ be the matrix of ϕ with the respect to the adapted base $\{e_0, ...e_n\}$. Then we define the matrix of Q on the reference R as

$M_R(Q) = [M_e(\phi)] \in P(M_{n+1}(\mathbb{K}))$. Note that it does not depend on the choice of the adapted basis or the representative of Q.

Let $Q = [\phi]$ be a quadric. Let M be a representative of $M_R(Q)$. Let $p = [x] \in \mathbb{P}$. Then we have that $p \in Q \Leftrightarrow \phi(x,x) = 0 \Leftrightarrow X_e^t M X_e = 0$. The last expression is the equation of Q on the reference R.

1.5 Dual projective spaces

In this subsection we will see a brief introduction to the duality of projective spaces. Let (P, E, π) be a projective space.

Definition 1.9. We will call dual projective space to the set $\mathbb{P}^* = \{H | H \text{ is a hyperplane of } P\}$

Note that we can give to P^* the structure of a projective space: $(\mathbb{P}^*, E^*, \pi^*)$ where E^* is the dual of E and $\pi^* : E^* \longrightarrow \mathbb{P}^*$ defined by $\pi^*(w) = \pi(ker(w) - \{0\})$. It is easy to see this. If E has finite rank then $rank(E) = rank(E^*)$ and this implies $dim(\mathbb{P}^*) = dim(\mathbb{P})$.
Suppose that E has rank n. Let F be a vector subspace of E. We define $F^\perp = \{w \in E^* | F \subset ker(w)\}$. It is clear that $F^\perp$ is a subspace of E^* of rank $n - rank(F)$. Let G be subspace of E^*. We define $G^\perp = \cap_{w \in G - \{0\}} ker(w)$. It is clear that $G^\perp$ is a subspace of E of rank $n - rank(G)$.
We will denote by $SE_d(E)$ the set of subspaces of E of rank d and we will denote by $Vlp_d(\mathbb{P})$ to the projective subspaces of $\mathbb{P}$ of dimension d.

Proposition 1.10. *We have the following bijection for* $0 \leq d \leq n$*:*

$$\begin{array}{ccc} SE_d(E) & \leftrightarrow & SE_{n-d}(E^*) \\ F & \rightarrow & F^\perp \\ G^\perp & \leftarrow & G \end{array}$$

Proof. The maps are well defined because the rank is the correct one. We have to prove that they are inverse maps. We have to check that $(F^\perp)^\perp = F$ and $(G^\perp)^\perp = G$. Because of the definition we have $(F^\perp)^\perp \subset F$ and $(G^\perp)^\perp \subset G$. Since the subspaces have the same rank we get the equality. □

Note that for every subspaces $F, G \in SE_d(E)$ we have the relation $F \subset G \Leftrightarrow G^\perp \subset F^\perp$ and for every subspaces $F, G \in SE_d(E^*)$ we have $F \subset G \Leftrightarrow G^\perp \subset F^\perp$.

Suppose that $\mathbb{P}$ has dimension n. Using the bijection between the subspaces of E and the projective subspaces of $\mathbb{P}$. We can get the following correspondence between $Vlp_d(\mathbb{P})$ and $Vlp_{n-d-1}(\mathbb{P}^*)$:

$$\begin{array}{ccccccc} Vld_d(\mathbb{P}) & \leftrightarrow & SE_{d+1}(E) & \leftrightarrow & SE_{n-d}(E^*) & \leftrightarrow & Vlp_{n-d-1}(\mathbb{P}^*) \\ L = [F]_\pi & \rightarrow & F & \rightarrow & F^\perp & \rightarrow & [F^\perp]_{\pi^*} =: L^* \\ W^* := [G^\perp]_\pi & \leftarrow & G^\perp & \leftarrow & G & \leftarrow & W = [G]_{\pi^*} \end{array}$$

This correspondence has the following properties:

$$L_1 \subset L_2 \Leftrightarrow L_2^* \subset L_1^*$$

$$(L_1 \cap L_2)^* = L_1^* + L_2^*$$

$$(L_1 + L_2)^* = L_1^* \cap L_2^*$$

for every $L_1, L_2 \in Vlp_d(\mathbb{P})$. I won't prove this relations because they are an immediate consequence of the same relation for the orthogonal subspaces. These relations will help us in the future for example to know what set is in $\mathbb{P}^*$ the set of hyperplanes H such that contains two points of $\mathbb{P}$:

$$p, q \in H \Leftrightarrow p + q \subset H \Leftrightarrow H = H^* \subset (p + q)^* = p^* \cap q^*$$

This tells us that this set is the intersection of p^* and q^*, that it corresponds to the intersection of two different hyperplanes of $\mathbb{P}^*$. This implies that it will be a projective subspace of $\mathbb{P}^*$ of dimension $n - 2$.

2. Finite geometry

In this section we are going to study projective spaces over a finite field and incidence structures which define projective planes.

2.1 Finite Projective Spaces

In this subsection we will see some general definitions of finite geometry that we will use in this thesis. The following definition constructs the space in which we will generally work.

Definition 2.1. Let $\mathbb{F}_q$ be the finite filed of cardinal $q = p^n$. Let $V(n, q)$ the vector space over field $\mathbb{F}_q$ of rank n consisting on n-tuples of this field. We denote $P(V(n+1, q))$ as $PG(n, q)$.

Because of we are working in spaces of finite cardinal we can count the number of subspaces of a vector space. The following definition is about it:

Definition 2.2. Let $\begin{bmatrix} n \\ k \end{bmatrix}_q$ be the number of subspaces of rank k of $V(n, q)$.

It will be very useful to have an easy way to calculate this number. The next proposition gives us a formule to calculate it:

Proposition 2.3. *We have the following formula:*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^n - q)...(q^n - q^{k-1})}{(q^k - 1)(q^k - q)...(q^k - q^{k-1})}$$

Proof. The number of k-tuples linearly independent of vector space of rank n is

$$(q^n - 1)(q^n - q)...(q^n - q^{k-1})$$

Because firstly we can choose $q^n - 1$ non trivial vectors. The vector that we choose expand a subspace of cardinal q. Then only we can choose from $q^n - q$ vectors, linearly independent with the first. If we iterate it we get the last expression. The main expression follows from the number of subspaces of rank k is the number of k-tuples of $V(n, q)$ divided by the number of k-tuples of $V(k, q)$. □

Proposition 2.4. *The number of subspaces of rank k through a given subspace of rank $d \leq k$ is $\begin{bmatrix} n-d \\ k-d \end{bmatrix}_q$.*

Proof. Let H be the subspace of rank k given. We have a bijection between the subspaces of $V(n, q)$ which contain H and the subspaces of $V(n, q)/H$. And we can add in this bijection that the subspaces will have rank k and $k - d$. It says that it is the same counting the subspaces of rank k through H or counting the subspaces of rank $k - d$ of $V(n, q)/H$. The last subspace is isomorphic to $V(n - d, q)$. □

Now we define the number of points of a projective space.

Definition 2.5. Let $\Theta_n(q)$ be the number of points of $PG(n, q)$.

The number of points of $PG(n, q)$ is exactly the same of the number of subspaces of rank 1 of $V(n+1, q)$. Using the proposition 2.3 it is $\begin{bmatrix} n+1 \\ 1 \end{bmatrix} = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + ... + q + 1$.

Now we will see a definition that talks about all possible cardinal of intersection between a set and hyperplane. We will use this in the section on scattered spaces:

Definition 2.6. Let T be a subset of $PG(n,q)$. If T intersects to all hyperplanes of $PG(n,q)$ in m_1, m_2,..., m_{i-1} or m_i points we will say that T is a i-intersection set with respect to hyperplanes with numbers of intersection $m_1, ..., m_i$.

Note that because every subset of $PG(n,q)$ is finite all subsets will be i-intersection sets with respect to hyperplanes where i is the cardinal of the set. For this reason we will be interested in this definition when i is small. A good example of this are the lines of $PG(n,q)$. Since the intersection of a line and a hyperplane has one point if and only if the line are not contained this implies that all lines are 2-intersection sets with intersection numbers $1, q+1$.

2.2 Projective planes

Definition 2.7. We will say $\Gamma = (P, L)$ is an incidence structure if L is a set of non-empty subsets of P. We say P is the set of points of Γ and L is the set of lines. We impose the condition that the set P is finite.

Definition 2.8. Let $\Gamma = (P, L)$ be an incidence structure. We define the dual of Γ as $\Gamma^* = (L, M)$ where $\forall x \in P$ we have a line $m_x \in M$ such that $x \in l \Leftrightarrow l \in m_x$.

Definition 2.9. Let $\Gamma = (P, L)$ be an incidence structure. We say that Γ is a projective plane if it has the following properties:

1. Every two points are incident with a unique line.
2. Every two lines are incident with a unique point.
3. There are four points, no three collinear.

It is easy to see that $PG(2,q)$ is a incidence structure with these three properties. Another observation is that the dual incidence structure of a projective plane is a projective plane. Now we call projective plane two objects: a projective space of rank 2 or an incidence structure with these three properties. It is very important to distinguish between which we are talking about.

Proposition 2.10. *In every finite projective plane $\Gamma = (P, L)$ there exists an $n \in \mathbb{N}$ such that every point is incident with $n+1$ lines. Duality every line is incident with $n+1$ points. We will say that this n is the order of the projective plane.*

Proof. Let K_l be the number of incident points to line l. Let R_p be the number of lines incident to point p.
To prove this, take two arbitrary points. We will see that they have the same number of incident lines. Let $p, q \in P$ for the axiom 3 of projective planes there are $r, s \in P$ which no three are collinear. In particular the line l joining r, s does not contain p and q. For each point in the line l, from axiom 1, we can join it to point p. This implies that $R_p \geq K_l$. Using axiom 2, each line incident with P is incident with l, which implies $R_p \leq K_l$. Applying the same argument to q we get $R_p = K_l = R_q$.
By duality we have the same property to lines and n is the same because we have $K_l = R_p$. □

Proposition 2.11. *A projective plane of order n has $n^2 + n + 1$ points and $n^2 + n + 1$ lines.*

Proof. We take a point p. This point is connected to all points of the projective plane and it is connected to each point only by one line. This point is incident with $n+1$ lines and each line has n points more. Counting this we have $n(n+1)+1 = n^2+n+1$ points. Applying the same arguement to the lines, for duality we have there are n^2+n+1 lines. □

$PG(2,q)$ has order q. To check it we can calculate $\begin{bmatrix}2\\1\end{bmatrix}_q = q+1$. It means each projective line has $q+1$ points.

2.3 Maximum distance separable codes and arcs

In this subsection I want to motivate the reader to study arcs in $PG(2,q)$ by showing an application in coding theory.

Definition 2.12. A code of length n is a subset of the set of n-tuples (called code-words) of a set (called the alphabet).

We can define the distance between two code-words like $d(x,y) = |\{i|x_i \neq y_i\}|$. Let C_n be a code of length n, the minimum distance of C_n is $\min\{d(x,y)|x,y \in C_n, x \neq y\}$.
A code with minimum distance at least $2e+1$ can correct up to e errors. We say that the code is an e-error correcting code.

Proposition 2.13. *Suppose that the alphabet of a code of length n has size a. If the minimum distance is d then the code has size at most a^{n-d+1}.*

Proof. Suppose that there are more than a^{n-d+1} words. Take any $n-d+1$ coordinates. There are a^{n-d+1} ways of build this coordinates with entries from the alphabet and there are more than a^{n-d+1} in the code. This implies that there are two words with the same entries in this coordinates. As a consequence the distance between these words is at most $d-1$. □

A code with size n over an alphabet of size a with minimum distance d such that has a^{n-d+1} code-words is called a maximum distance separable code or MDS-code.

Definition 2.14. A linear code C is a code with alphabet $\mathbb{F}_q$ and the set of codewords is a subspace of $V(n,q)$. Let k be the rank of the subspace. We say that C is a $[n,k,d]$-code.

Because of the proposition 2.13 we have $k \leq n-d+1$. A $[n, n-d+1, d]$-code is a MDS-code.

Let x be a codeword. The number of non-zero entries is called the weight of the codeword and we write $wt(x)$.The minimum weight of the non-zero code-words of a code we will say is the minimum weight of the code.

Proposition 2.15. *Let C be a linear code. Then the minimum weight of C is equal to the minimum distance of C.*

Proof. We write d for the minimum distance and w for the minimum weight. Since C is linear we can get the following relations:

$$d(x,y) = wt(x-y), wt(x) = d(x,0)$$

For the first relation we know that $w \leq d$. And because of the second $d \leq w$. □

Definition 2.16. An arc is a subset of $PG(r,q)$ which contains at least $r+1$ points such that each hyperplane is incident to the arc in at most r points.

We are going to enunciate two propositions that will make a correspondence between arcs and linear codes. It is a good reason to study arcs.

Proposition 2.17. *We can make an arc of $PG(n-d,q)$ with number of points between $n-d+1$ and n using a MSD $[n, n-d+1, d]$-code.*

Proof. Let C be a MSD $[n, n-d+1, d]$-code. In order to make the proof clearer we define $k = n-d+1$. Let $c_1, ..., c_k$ a basis of C. We can take $a_1, ..., a_n \in V(k,q)$ such that $(a_j)_i = (c_i)_j$. The set $A = \{[a_j] | j = 1, ..., n\}$ has at least k points because the matrix $\{a_j\}$ has rank k because $\{c_i\}_{i=1,...,k}$ is a basis. We are going to prove that A is an arc. We only have to prove that each hyperplane of $PG(k-1,q)$ intersects A at most $k-1$ points.
Take an arbitrary hyperplane of $PG(k-1,q)$: $\sum_{i=1}^{k} \alpha_i x_i = 0$. Then we have:

$$(\sum_{i=1}^{k} \alpha_i c_i)_j = \sum_{i=1}^{k} \alpha_i (c_i)_j = \sum_{i=1}^{k} \alpha_i (a_j)_i = 0$$

This relation says us that the number of points that are incident with the hyperplane is the same of the cardinality of the set $\{j | (\sum_{i=1}^{k} \alpha_i c_i)_j = 0\}$. We know that the code C has minimum weight d. This implies that the number of j is at most $n-d = k-1$. □

Proposition 2.18. *Let A be an arc with n points of $PG(r,q)$. Using A we can make a MDS $[n, r+1, d]$-code with d at most $n-r$. .*

Proof. Firstly we make a code in the following way: We can suppose that $A = \{[a_j] | j = 1, ..., n\}$ and define $(c_i)_j = (a_j)_i$. We want to prove that $\{c_i\}$ spans a space of rank $r+1$ in $V(n,q)$. The points of A are not contained in a hyperplane of $PG(r,q)$ which means that his representatives span all $V(r+1,q)$. By construction the rank of the matrix $\{c_i\}$ is $r+1$. Defining the code $C =< c_i >_{i=1,...,n}$ we have that C is a $[n, r+1, d]$-code. To prove the proposition we only have to check that the maximum weight of the code C is $n-r$. Using the main relation of the proposition 2.17:

$$(\sum_{i=1}^{k} \alpha_i c_i)_j = \sum_{i=1}^{k} \alpha_i (c_i)_j = \sum_{i=1}^{k} \alpha_i (a_j)_i = 0$$

It says us that the minimum weight of the code C is at most n minus the maximum number of points contained in one hyperplane. Because of this we have $d \leq n-r$. □

We are going to give an explicit arc:

Proposition 2.19. *The set of points of the $PG(r,q)$ $A = \{[(1, t, ..., t^r)] | t \in \mathbb{F}_q\} \cup \{[(0, ..., 0, 1)]\}$ is an arc with $q+1$ points.*

Proof. It is easy to check that A has $q+1$ points because all the representatives are linearly independent. Let $\alpha_0 x_0 + ... + \alpha_r x_r = 0$ be the equation of an hyperplane.
Suppose that $\alpha_r \neq 0$. The equation $\alpha_0 + \alpha_1 t + ... + \alpha_r t^r = 0$ has at most r solutions. This implies that the hyperplane has at most r points with the form $[(1, t, ..., t^r)]$ and because of $\alpha_r \neq 0$ [(0,...,0,1)] isn't in

the hyperplane.
Suppose that $\alpha_r = 0$. Then $[(0, ..., 0, 1)]$ is in the hyperplane but the equation $\alpha_0 + \alpha_1 t + ... + \alpha_{r-1} t^{r-1}$ has at most $r - 1$ solutions. □

The next proposition is about the size of arcs, a very important issue to study.

Proposition 2.20. *Let A be an arc of $PG(r, q)$ then $|A| \leq q + r$.*

Proof. Take a subset S of A with $r-1$ points. S is a subset of $PG(r, q)$ which spans a projective subspace L of dimension $r - 2$. If not, we can add points of A so that we have $r + 1$ points in the same hyperplane and we will have a contradiction because A is an arc.
We can count the hyperplanes through L using proposition 2.4 with $d = n - 2, k = n - 1$. It give us that there are $q + 1$ hyperplanes through L. Each hyperplane that contains S contains at most one other point of $A - S$, and each point of $A - S$ is contained in a hyperplane which contains S. Thus we have $|A| \leq r - 1 + q + 1 = r + q$. □

3. Ovals

In this section we will study the ovals of a projective plane seen as an incidence structure. And then we will see that ovals in $PG(2,q)$, q odd, are given by a quadratic equation, this is the main theorem of this section, Segre's theorem.

3.1 Ovals

Definition 3.1. Let $\Gamma = (P, L)$ be a projective plane of order q. We will say that a subset $A \subset P$ is an oval if it has size $q+1$ and every line of Γ is incident at most to two points of A.

We can take a point P of an oval. This point is incident with $q+1$ lines, q of them are incident with another point of the oval. The last line is only incident with P. We will call it the tangent to P. An oval has $q+1$ tangents, one for each point.

In $PG(2,q)$ it is equivalent the definition of an oval or an arc of size $q+1$. In $PG(2,q)$ we have the example of the conics. Recall that a conic is a subset of $PG(2,q)$ defined by a quadratic equation. For each non-degenerate conic we can find a projective reference so that the equation is $x^2 = yz$.

$$C = \{[(x,y,z)] | x^2 = yz\} = \{[(0,1,0)]\} \cup \{[(t,t^2,1)] | t \in \mathbb{F}_q\}$$

It is easy to see that C has $q+1$ points. Since C is defined by a quadratic equation, each line of $PG(2,q)$ is incident with C at most 2 times.

I will give an other example in $PG(2,q)$:

Proposition 3.2. *The set*

$$A = \{[(1,t,t^{2^i})] | t \in \mathbb{F}_q\} \cup \{[(0,0,1)]\}$$

is an oval in $PG(2,q)$, $q = 2^h$ *if* $mcd(i,h) = 1$.

Proof. A has $q+1$ points. We only have to check that every line in $PG(2,2^h)$ is incident at most two points of A:
There are q lines incident to $[(0,0,1)]$ of the form $y = ax$. Each line is incident to $[(1,a,a^{2^i})]$. It is clear that the last line incident to $[(0,0,1)]$ is $x = 0$ and it is the tangent of this point. We have counted all lines incident to this point. Now I am going to study the lines of the form $z = ax + by$. Fix a line $L : z = ax + by$. Firstly note that exponents in the field $\mathbb{F}_q$ are defined in $\mathbb{Z}/\mathbb{Z}_{q-1}$. I will see that if we have two distinct points incident to L of the form $[(1,u,u^{2^i})]$ and $[(1,v,v^{2^i})]$ then we have $u - v = b^m$ where $m = (2^i - 1)^{-1}$. It means that the difference of the parameter of two points of A incident with L only depends on L. This tells us that there are at most two points in A that are incident to L.
Suppose that $[(1,u,u^{2^i})]$ and $[(1,v,v^{2^i})]$ are in L. Then we have $u^{2^i} = a + bu$ and $v^{2^i} = a + bv$. Since the field has characteristic 2 we can write $(u-v)^{2^i} = u^{2^i} - v^{2^i} = b(u-v)$ and $u - v \neq 0$ because the points are different. The equation is $(u-v)^{2^i-1} = b$. By the hypothesis $mcd(i,h) = 1 \Rightarrow mcd(2^i-1, q-1) = 1$ and using Bezout we get that $\exists m, n \in \mathbb{Z}$ such that $m(2^i-1) + n(q-1) = 1$ that in $\mathbb{Z}/\mathbb{Z}_{q-1}$ is $m(2^i-1) = 1$. Then using this: $b^m = (u-v)^{(2^i-1)m} = u - v$. □

We are going to prove a very beautiful result which says if we have an oval then each point of the plane is incident to zero or two tangents.

Proposition 3.3. *Let $\mathcal{O}$ be an oval in a projective plane of order q, q odd. Then every point of the projective plane not in $\mathcal{O}$ is incident with zero or two tangents of $\mathcal{O}$.*

Proof. Let x_i be the number of points not in $\mathcal{O}$ such that are incident with i tangents of $\mathcal{O}$.
Fix a point $p \notin \mathcal{O}$. Suppose that p is incident with an odd number of tangents. Then the number of points of $\mathcal{O}$ is odd, since the other lines incident with p are incident with an even number of points of $\mathcal{O}$. However, $q+1$ is even, so p is incident with an even number of tangents, so $x_i = 0$ if i is odd.
We are going to count the pairs (p, l) where l is a tangent of $\mathcal{O}$ and $p \in l - \mathcal{O}$ in two different ways: Take a tangent l have q points not in $\mathcal{O}$. There are $q+1$ tangents in $\mathcal{O}$, consequently the number of pairs is $q(q+1)$. If we calculate joining the points on the number of tangents we get that the number of pairs is $\sum_{i\geq 2} ix_i$. So the equation is $\sum_{i\geq 2} ix_i = q(q+1)$.
Now, we are going to count the triples (p, l, m) such that l and m are different tangents of $\mathcal{O}$ and $p \in l \cap m$ in two different ways:
Note that if $p \in l \cap m$ then $p \notin \mathcal{O}$ because there is only one tangent incident with each point of the oval. Taking $p \notin \mathcal{O}$ such that is in i tangents then we can choose $i(i-1)$ triples. Then we have the number of triples is $\sum_{i\geq 2}(i-1)x_i$. Fix l tangent of $\mathcal{O}$, then all the other q tangents intersect l once. Since there are $q+1$ tangents the number of triples is $q(q+1)$. So we can get that $\sum_{i\geq 2} i(i-1)x_i = q(q+1)$. Combining the two last equations we have:

$$\sum_{i\geq 2} i(i-2)x_i = 0$$

All terms of the sum are non-negative, so $x_i = 0$ if $i \neq 0, 2$. □

3.2 Segre's theorem

Now we are going to prove Segre's theorem, which was proven by Beniamino Segre in 1955 [5]. The proof given here is adapted from [2]. It is the main theorem of this section because it says that when q is odd, in $PG(2, q)$, an oval and a conic are the same thing.

Theorem 3.4. *An oval in $PG(2, q)$, q odd, is a conic.*

Proof. We are going to prove it building a quadratic equation that contains all points of the oval. Then the set defined by it will be the oval because both have $q+1$ points. Let $[x], [y], [z]$ be three different points of $\mathcal{O}$. We take the basis x, y, z of $V(3, q)$. It is a basis because $\mathcal{O}$ is an oval.
The tangents to the points $[x], [y], [z]$ are $\alpha_{21}X_2 + \alpha_{31}X_3 = 0$, $\alpha 12X_1 + \alpha_{32}X_3 = 0$, $\alpha_{13}X_1 + \alpha_{23}X_2 = 0$ respectively.
Let $[s] \in \mathcal{O} - \{[x], [y], [z]\}$ where $s = (s_1, s_2, s_3)$ on the basis $\{x, y, z\}$. Then we can consider the line joining $[s]$ and $[z]$: $s_2X_1 - s_1X_2 = 0$. Because the property of the ovals all lines are different, so the following set has all no null elements of $\mathbb{F}_q$:

$$\left\{ \frac{s_2}{s_1} | [s] \in \mathcal{O} - \{[x], [y], [z]\} \right\} \cup \left\{ \frac{-\alpha_{13}}{\alpha_{23}} \right\}$$

Using it we have:

$$-\frac{\alpha_{13}}{\alpha_{32}} \prod_{[s]\in\mathcal{O}-\{[x],[y],[z]\}} \frac{s_2}{s_1} = -1 \tag{1}$$

I define the following linear maps on basis $\{x, y, z\}$: $T_x(X) = \alpha_{21}X_2 + \alpha_{31}X_3$, $T_y(X) = \alpha_{12}X_1 + \alpha_{32}X_3$, $T_z(X) = \alpha_{13}X_1 + \alpha_{23}X_2$. It is easy to see that $T_z(x) = \alpha_{31}$ and $T_z(y) = \alpha_{32}$. Using (1) this implies $T_z(x)\prod s_2 = T_z(y)\prod s_1$. Similarly we can obtain $T_x(y)\prod s_3 = T_x(z)\prod s_2$ and $T_y(z)\prod s_1 = T_y(x)\prod s_3$. Combining this we get:

$$T_x(y)\,T_y(z)\,T_z(x) = T_x(z)\,T_y(x)\,T_z(y) \tag{2}$$

Let $[v], [u], [w]$ three different points of $\mathcal{O} - \{[x]\}$. By interpolation, we can verify the following equation evaluating in $X = v$ and $X = u$ because in both sides are polynomials of degree 1:

$$T_x(X) = T_x(u)\frac{\det(X, u, x)}{\det(u, v, x)} + T_x(v)\frac{\det(X, u, x)}{\det(v, u, x)}$$

Evaluating this in $X = w$ we get:

$$T_x(w)\det(u, v, x) + T_x(v)\det(w, u, x) + T_x(u)\det(v, w, x) = 0 \tag{3}$$

Changing the rolls of x, u, v, w we can obtain the following three equations:

$$T_u(w)\det(x, v, u) + T_u(v)\det(w, x, u) + T_u(x)\det(v, w, u) = 0$$

$$T_v(w)\det(x, u, v) + T_v(u)\det(w, x, v) + T_v(x)\det(u, w, v) = 0$$

$$T_w(u)\det(x, v, w) + T_w(v)\det(u, x, w) + T_w(x)\det(v, u, w) = 0$$

Using (2) we get the following relation:

$$\frac{T_w(x)}{T_x(w)} = \frac{T_w(u)\,T_u(x)}{T_x(u)\,T_u(w)} = \frac{T_w(v)\,T_v(x)}{T_x(v)\,T_v(w)}$$

Multiplying it by (3) then we have the following equation:

$$T_w(x)\det(u, v, x) + T_v(x)\frac{T_w(v)}{T_v(w)}\det(w, v, x) + T_u(x)\frac{T_w(u)}{T_u(w)}\det(v, w, x) = 0$$

Using the three equations following (3) we can change $T_w(x)$, $T_v(x)$ and $T_u(x)$ from the last one and we obtain:

$$\begin{aligned}
&\det(u, v, x)(\,T_w(u)\det(x, v, w) + T_w(v)\det(u, x, w)) \\
&+\frac{T_w(v)}{T_v(w)}\det(w, u, x)(\,T_v(w)\det(x, u, v) + T_v(u)\det(w, x, v)) \\
&-\frac{T_w(v)}{T_u(w)}\det(v, w, x)(\,T_u(w)\det(x, v, u) + T_u(v)\det(w, x, u)) = 0
\end{aligned}$$

and rearranging the last coefficient using (2):

$$2\,T_w(u)\det(u, v, x)\det(x, v, w) + 2\,T_w(v)\det(u, v, x)\det(u, x, w) + 2\,T_v(u)\frac{T_w(v)}{T_v(w)}\det(w, u, x)\det(w, x, v) = 0$$

Now with the basis $\{u, v, w\}$ we have that an arbitrary point $[x] \in \mathcal{O}$ satisfies the equation:

$$2\,T_w(u)x_3x_1 + 2\,T_w(v)x_3x_2 + 2\,T_v(u)\frac{T_w(v)}{T_v(w)}x_2x_1 = 0$$

We have to check that this equation is a non degenerate quadratic form. All the coefficients are different from 0 because the characteristic of the field isn't 2 and there are no other point of the oval in a tangent. There we use the hypothesis that q is odd. □

4. Kestenband

In this section we are going to see the construction of an arc of size $q - \sqrt{q} + 1$ in $PG(2, q)$ that it is not contained in a conic. This arc was found by Kestenband [3]. In this section firstly we will study the hermitian curves which we will use in the construction.

4.1 Hermitian curves

Definition 4.1. Let β be a map in $V = V(n, q)$ such that $\beta : V \times V \longrightarrow \mathbb{F}_q$ and let σ be automorphism of $\mathbb{F}_q$ such that $\sigma^2 = 1$ and $\sigma \neq 1$. We will say that β is an hermitian form if it have the following properties:

1. $\beta(u + w, v) = \beta(u, v) + \beta(w, v)$
2. $\beta(u, v + w) = \beta(u, v) + \beta(u, w)$
3. $\beta(au, bv) = ab^{\sigma}\beta(u, v)$
4. $\beta(u, v) = \beta(v, u)^{\sigma}$

Note that the existence of σ implies that q must be a square. Then because of Galois theory σ is unique and $x^{\sigma} = x^{\sqrt{q}}$ and the fixed field of σ is $\mathbb{F}_{\sqrt{q}}$. For this reason we can say that $\forall u \in \mathbb{F}_q, \beta(u, u) \in \mathbb{F}_{\sqrt{q}}$. We will say β is degenerate if there exists $w \neq 0$ such that $\beta(w, u) = 0\ \forall u \in V(n, q)$. A vector u is isotropic to β, a non-degenerate hermitian form, if $\beta(u, u) = 0$ and a pair $\{u, v\}$ is said hyperbolic if $\beta(u, v) = 1$ and u, v are isotropic. A subspace U is anisotropic if $\beta(u, u) \neq 0, \forall u \in U - 0$.

We prove some lemmas that will help us to determinate the equation of an hermitian curve. These lemmas can be found in [1].

Lemma 4.2. *Suppose that L is a subspace of rank 2 of $V(n, q)$ that contains an isotropic vector to β, a hermitian form. Then β restricted to L is degenerate or has an hyperbolic pair $\{u, v\}$ such that $L =< v, u >$.*

Proof. If β restricted to L is non-degenerate then there exists $w \in V(n, q)$ such that $\beta(u, w) \neq 0$. If $\beta(w, w) = 0$ we have finished the proof by scaling w appropriately. Suppose that $\beta(w, w) \neq 0$. Take d such that $d^{\sigma} \neq -d$. There exists such a d since the change of sign is not a morphism if the characteristic is different of 2 and if it is 2, it is the identity. We can define $c := \frac{d^{\sigma}\beta(w,w)}{d+d^{\sigma}}$. Then $c + c^{\sigma} = \beta(w, w)$. Define $a := \beta(w, w)$ and take $v = -a^{-1-\sigma}cu + a^{-\sigma}w$. □

Lemma 4.3. *Let β be a non-degenerate hermitian form of $V(n, q)$. Let W be a maximal totally isotropic subspace and suppose that it has rank r.*
Then exists a basis $\{e_i | i = 1, ..., r\} \cup \{f_i | i = 1, ..., r\}$ of a subspace $X \subset V$ such that $W =< e_1, ..., e_r >$ and $V = X \oplus U$. Moreover (e_i, f_i) is an hyperbolic pair.

Proof. If we have $r = 0$ then we have finished.
Suppose that $r > 0$, then exists $e_1 \in W$ that is isotropic. Since β is non-degenerate, there exists $v \in V$ such that $\beta(e_1, v) \neq 0$ and β restricted to $< e_1, v >$ is non-degenerate. By Lemma 4.2 we have that there exists a hyperbolic pair $\{e_1, f_1\}$ such that $V =< e_1, f_1 > \oplus V_1$ where $V_1 =< e_1, f_1 >^{\perp}$.
Define $W_1 = W \cap V_1$. We can calculate the rank of W_1 by Grassman:

$$rank(W_1) = rank(W \cap V_1) = rank(W) + rank(V_1) - rank(W \oplus V) = r + (n - 2) - (n - 1) = r - 1$$

It is not difficult to check that $rank(W \oplus V_1) = n-1$. If β restricted to V_1 is degenerate then there exists $u \in V_1 - \{0\}$ such that $\beta(u, w) = 0\ \forall w \in V_1$. Since $\beta(u, v) = 0\ \forall v \in < e_1, f_1 >$ then β will be degenerate in V. This implies that β is non-degenerate in V_1.
Then applying the same to the spaces V_1 and W_1, which is totally isotropic, we are finished by induction. □

The next lemma tell us that if the rank of subspace is more than 2 then the maximal isotropic space is non-trivial. This is important because it allows us to apply the last lemma to find a basis such that the form has an easy expression.

Lemma 4.4. *Let β be a non-degenerate hermitian form of $V(n, q) = V$. If V has at least rank 2, V will have an isotropic vector.*

Proof. Suppose that v is not an isotropic vector and define $b = \beta(v, v) \in \mathbb{F}_{\sqrt{q}}$. Take $u \in < v >^{\perp}$ and consider $\beta(u + av, u + av) = \beta(u, u) + a^{\sigma+1}\beta(v, v)$. Since $-\frac{\beta(u,u)}{b} \in \mathbb{F}_{\sqrt{q}}$ and the map $f : \mathbb{F}_q \longrightarrow \mathbb{F}_{\sqrt{q}}$ such that $f(x) = x^{\sigma+1}$ is surjective. Using it we can take $a \in \mathbb{F}_q$ so that $a^{\sigma+1} = -\frac{\beta(u,u)}{b}$. Then the vector $u + av$ is isotropic.
We only have to check that f is surjective. Firstly we can see that $|f^{-1}(a)| \leq \sqrt{q} + 1$ because this set is defined by polynomial of degree $\sqrt{q}+1$. Suppose that exists $a \in \mathbb{F}_{\sqrt{q}}$ such that $f^{-1}(a) = \emptyset$. Then we can get the following contradiction:

$$q = |\mathbb{F}_q| = |\cup_{c \in \mathbb{F}_{\sqrt{q}} - \{a\}} f^{-1}(c)| = \sum_{c \in \mathbb{F}_{\sqrt{q}} - \{a\}} |f^{-1}(c)| \leq (\sqrt{q} - 1)(\sqrt{q} + 1) = q - 1$$

□

Let β be a non-degenerate hermitian curve. By Lemma 4.4 we know that an anisotropic space has rank 1 or 0. Suppose that V has rank n. By the lemma 4.3, we can find a basis such that $\beta(u, v) = u_1 v_2^{\sigma} + u_2 v_1^{\sigma} + ... + u_{n-1} v_n^{\sigma} + u_n v_{n-1}^{\sigma}$ if n is even and $\beta(u, v) = u_1 v_2^{\sigma} + u_2 v_1^{\sigma} + ... + u_{n-2} v_{n-1}^{\sigma} + u_{n-1} v_{n-2}^{\sigma} + u_n v_n^{\sigma}$ if n is odd.

Let $H = \{[x] \in PG(n, q) | \beta(x, x) = 0\}$ where β is a hermitian form in $PG(n, q)$. We will call it a hermitian surface. Now I am interested to know how many points it has. We will say that H is non-degenerate if β is non-degenerate.

Proposition 4.5. *Let H be a non-degenerate hermitian curve of $PG(2, q)$. Let L be a line. If $H \cap L$ has at least two points then it has $\sqrt{q} + 1$ points.*

Proof. The two points, that the intersection has, are $[x]$, $[y]$. Let h be the hermitian form associate to the curve. All the points of the line are $\{[x]\} \cup [x + \lambda y]\}_{\lambda \in \mathbb{F}_q}$. We can define a map such that $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_{\sqrt{q}}$ where $\phi(\lambda) = h(x + \lambda y, x + \lambda y) = \lambda h(x, y) + \lambda^{\sqrt{q}} h(x, y)$. It is clear that all points of the intersection are $[y]$, which are associated with one $\lambda \in \phi^{-1}(0)$.
Suppose that $h(x, y) \neq 0$. For each $a \in \mathbb{F}_{\sqrt{q}}$, $\phi^{-1}(a)$ has at most $\sqrt{q}$ elements because it is defined by a polynomial of degree $\sqrt{q}$. Now we are going to see that it is exactly $\sqrt{q}$:

$$q = |\mathbb{F}_q| = |\cup_{a \in \mathbb{F}_{\sqrt{q}}} \phi^{-1}(a)| = \sum_{a \in \mathbb{F}_{\sqrt{q}}} |\phi^{-1}(a)| \leq \sum_{a \in \mathbb{F}_{\sqrt{q}}} \sqrt{q} = \sqrt{q}\sqrt{q} = q$$

This equation implies that all must be equal. Then we have that $|\phi^{-1}(0)| = \sqrt{q}$. We have seen that the intersection has $\sqrt{q} + 1$ points.

Suppose that $h(x,y)=0$. This implies that all points of the line are in H. Since L has dimension 1, this contradicts Lemma 4.3. □

Now, by counting, we can calculate the number of points of a hermitian curve in $PG(2,q)$. To prove it we only need an extra lemma, which says that for every point of an hermitian curve has only one tangent (line that only intersects in one point to the curve). We will prove this later.

Corollary 4.6. *A non-degenerate hermitian curve in $PG(2,q)$ has $q\sqrt{q}+1$ points.*

Proof. Let H be the curve. We are going to prove it by double counting. We count pairs (p,l), where $p\in H$ and l is a line of $PG(2,q)$ for which $l\ni p$, in two ways.
Firstly fix the point. Each point is incident with $q+1$ lines. The number of pairs (p,l) is $|H|(q+1)$.
Finally fix the line. Let l be a line of $PG(2,q)$. This line intersects H in 1 or $\sqrt{q}+1$ points. In $PG(2,q)$ there are q^2+q+1 lines. There are $|H|$ tangents, which only intersect H in one point, and there are $q^2+q+1-|H|$ lines which intersect H in $\sqrt{q}+1$ points. This implies that the number of pairs is $(q^2+q+1-|H|)(\sqrt{q}+1)+|H|$. Combining these two counts, we get that $|H|=q\sqrt{q}+1$. □

Lemma 4.7. *Let H be a non-degenerate hermitian curve of $PG(2,q)$ represented by h. Let $L=[W]=<u,v>$ be a line such that u,v are isotropic vectors of h. Then $h_{|W}$ is non-degenerate.*

Proof. Suppose that $h_{|W}$ is degenerate. This implies that exists a vector $w\in W$ such that $h(w,w')=0$ for all $w'\in W$. Because of W has rank 2 we can suppose that $W=<u,w>$ and expressing $h_{|W}$ in this basis we have that is the 0 form. This implies that $H\cap L$ has $q+1$ points, contradicting Proposition 4.5. □

Lemma 4.8. *Let H be a non-degenerate hermitian curve in $PG(2,q)$ defined by the form h. For each $p\in H$ then $\exists!$ tangent of H through p.*

Proof. Let $p=[x]$ and $[y]\notin H$. The points of the line defined by $[x],[y]$ are $\{[y]\}\cup\{[x+\lambda y]\}_{\lambda\in\mathbb{F}_q}$.
Suppose that $h(x,y)\neq 0$. We can define a map $\phi(\lambda)=h(x+\lambda y,x+\lambda y)$ and proceeding similarly proposition 4.5 we obtain that this line has $\sqrt{q}+1$ points in H. Thus, it is not a tangent.
Suppose that $h(x,y)=0$. We have the equation $0=h(x+\lambda y,x+\lambda y)=h(x,x)+\lambda h(x,y)+\lambda^{\sqrt{q}}h(x,y)+\lambda^{\sqrt{q}+1}h(y,y)$. Since $[y]\notin H$ the only point of H on the line joining $[x]$ and $[y]$ is $[x]$. We have proved that if $h(x,y)=0$ and $[y]\notin H$ the line defined by $[x],[y]$ is a tangent through $[x]$. But all the points such that $0=h(x,y)=h(y,x)=y_1x_2^\sigma+y_2x_1^\sigma+y_3x_3^\sigma$ are incident with the same line. This line is the unique tangent to H through p. □

We are using that the curve is non-degenerate, so it will be useful to have a lemma that help us know when a hermitian form is non-degenerate:

Lemma 4.9. *Let M be a matrix such that $M^t=M^{\sqrt{q}}$, we will call a matrix hermitian with this property. Then the form defined by $\beta(x,y)=x^tMy^{\sqrt{q}}$ is a non-degenerate hermitian form if and only if* $\det(M)\neq 0$.

Proof. Define $f: V(n,q)\longrightarrow V(n,q)$ such that $f(x)=\begin{pmatrix}\beta(x,e_1)\\ \vdots\\ \beta(x,e_n)\end{pmatrix}$ where $e_1,\dots,e_n$ is the canonical basis of $V(n,q)$. This is a linear map with matrix M in the canonical basis. And we have:

$$\det M=0\Leftrightarrow ker(f)\neq\{0\}\Leftrightarrow\exists v\neq 0 \text{ such that } \forall u\in V(n,q)\ \beta(v,u)=0\Leftrightarrow\beta \text{ is degenerate}$$

□

4.2 The arc of Kestenband

The following theorem concerns the construction of an arc of size $q-\sqrt{q}+1$ that it is not contained in a conic:

Theorem 4.10. *Let $q>9$ be a square. Let I be the identity matrix and let H be a hermitian matrix. For any hermitian matrix M we define the following set:*

$$V(M)=\{[x]\in PG(2,q)|x^tMx^q=0\}$$

If the characteristic polynomial of H is irreducible over $\mathbb{F}_q$, then the set $S=V(I)\cap V(H)$ is an arc of $PG(2,q)$ that is not contained in a conic.

Proof. Since the characteristic polynomial of H is irreducible over $\mathbb{F}_q$, we have that $\det(H-\lambda I)\neq 0$ for every $\lambda\in\mathbb{F}_q$. Then the set $V(H+\lambda I)$ will be a non degenerate hermitian curve.
Take the curves $V_\lambda=V(H+\lambda I)$ for all $\lambda\in\mathbb{F}_{\sqrt{q}}$ and $V_\infty=V(I)$. If $[x]$ is at least in two curves V_a, then making linear combinations of the equations of these curves we find that $[x]$ is in all curves V_a. Suppose that $[x]\notin V(I)$ then we have $x^tHx^{\sqrt{q}}=a\in\mathbb{F}_{\sqrt{q}}$ and $x^tIx^{\sqrt{q}}=-b$ where $b\in(\mathbb{F}_{\sqrt{q}})^*$. Multiplying the second equation by $\frac{a}{b}$ and adding to the first we found that $[x]\in V(H+\frac{a}{b}I)$. Using this we know that every point is in all curves V_a or only in one.
Now we use double counting to calculate the size of the set. We will count the pairs (p,V) where $p\in PG(2,q)$ and V is one of previous curves such that $p\in V$. Fixing V we have that the number of pairs is $\sum|V|=\#$ hermitian curves $V\#$ points in hermitian curve $=(\sqrt{q}+1)(q\sqrt{q}+1)$. Now fixing p, if $p\in S$ then p is in all curves V and if $p\notin S$ then p is in exactly one curve V. So the number of pairs (p,V) is $|S|(\sqrt{q}+1)+q^2+q+1-|S|$. Using the two ways of counting we get that $|S|=q-\sqrt{q}+1$.
Now we will see that S is an arc. Let l be a line incident with $r\geq 2$ points of S. Then l intersects each curve V in $\sqrt{q}+1$ points, $\sqrt{q}+1-r$ of which are not in S. The number of points that are in l but not in S is $q+1-r$. Since each point of $l-S$ is incident with exactly one curve V,

$$q+1-r=(\sqrt{q}+1)(\sqrt{q}+1-r)$$

Hence, $r=2$. This proves that S is an arc.
We want to see that S is not a subset of a conic. We will use Bezout's theorem. Firstly we have to check that a conic and a hermitian curve don't share any component. We can assume that the conic is $y^2=xz$ and we take a general non-degenerate hermitian curve $h(x,y,z)$. We know that the conic is irreducible, this implies that if they share a component then the conic divides the hermitian curve. This says us that the polynomial h is 0 in $\frac{\mathbb{F}_q[X,Y,Z]}{<Y^2-XZ>}$. Using that a basis of this space is the residues of $\{YX^iZ^j,X^iZ^j\}_{i,j\geq 0}$ we get that the hermitian form is 0. A contradiction since it is non-degenerate. Using Bezout's theorem we get that S have at most $2\sqrt{q}+2$ points of the conic but $q-\sqrt{q}+1>2\sqrt{q}+2$ for $q>9$.

□

5. Baer lines and linear sets

5.1 Regulus

Definition 5.1. Let $\Sigma = PG(3, q)$. A regulus is a set R of $q+1$ disjoint lines of Σ such that every line that intersects at least with 3 lines of R intersects all $q+1$ lines of R.

Lemma 5.2. *For every three disjoint lines l_1, l_2, l_3 of $PG(n, q)$ there are at most $q+1$ lines such that intersects l_1, l_2 and l_3. Equivalently $\#\{m \text{ line of } PG(n,q) | m \cap l_i \neq \emptyset \text{ for } i = 1,2,3\} \leq q+1$.*

Proof. We have to check for every $p \in l_3$ there is at most one line m through p such that $m \cap l_2 \neq \emptyset$ and $m \cap l_3 \neq \emptyset$ because l_3 has $q+1$ points. Assume that $\exists$ m_1, m_2 different lines with the previous hypothesis. We will call $p_i = m_1 \cap l_i$ and $q_i = m_2 \cap l_i$ for $i = 1, 2$. The previous points are all different because l_1 and l_2 are disjoint and m_1 and m_2 are different lines. Let π be the plane defined by m_1 and m_2. This implies that $p_1, p_2, q_1, q_2 \in \pi$. Because of $l_1 = p_1 \wedge q_1$ and $l_2 = p_2 \wedge q_2$ we know that $l_1, l_2 \in \pi$. Every two lines in a projective plane have non-empty intersection. Hence $l_1 \cap l_2 \neq \emptyset$. We get a contradiction, since l_1 and l_2 are disjoint. □

This proposition will be very useful:

Proposition 5.3. *Given 3 disjoint lines of $\Sigma = PG(3, q)$ then $\exists!$ regulus such that contain these lines.*

Proof. We will call these three lines l_0, l_1, l_∞. We have to check that we can take a basis such that these lines have the following expression:

$$l_0 =< (0,0,0,1), (0,0,1,0) >, l_1 =< (1,0,0,1), (0,1,1,0) >, l_\infty =< (1,0,0,0), (0,1,0,0) >$$

Suppose that $l_0 =< v_1, v_2 >, l_1 =< u_1, u_2 >, l_\infty =< w_1, w_2 >$. Because of l_0 and l_∞ are disjoint $\{v_1, v_2, w_1, w_2\}$ is a basis. Hence we can write u_1, u_2 as a linear combination of these four vectors:

$$u_1 = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 w_1 + \lambda_4 w_2$$

$$u_2 = \mu_1 v_1 + \mu_2 v_2 + \mu_3 w_1 + \mu_4 w_2$$

Claim: The set $\{n_1 = \lambda_1 v_1 + \lambda_2 v_2, n_2 = \lambda_3 w_1 + \lambda_4 w_4, n_3 = \mu_1 v_1 + \mu_2 v_2, n_4 = \mu_3 w_1 + \mu_4 w_2\}$ is a basis. We have to check that they are linearly independent:

$$\gamma_1 n_1 + \gamma_2 n_2 + \gamma_3 n_3 + \gamma_4 n_4 = 0$$

Substituting the expressions of n_i and using that v_1, v_2, w_1, w_2 is basis we get the following linear system where the variables are γ_i:

$$\lambda_1\gamma_1 + \mu_1\gamma_3 = 0$$

$$\lambda_2\gamma_1 + \mu_2\gamma_3 = 0$$

$$\lambda_3\gamma_2 + \mu_3\gamma_4 = 0$$

$$\lambda_4\gamma_2 + \mu_4\gamma_4 = 0$$

To find $\gamma_i = 0$ we need that $\det(A) = (\mu_1\lambda_2 - \mu_2\lambda_1)(\lambda_3\mu_4 - \lambda_4\mu_3) \neq 0$. Firstly we will check that $\mu_1\lambda_2 - \mu_2\lambda_1 \neq 0$. Suppose $\mu_1\lambda_2 - \mu_2\lambda_1 = 0$. Then we have $\mu_1\lambda_2 = \mu_2\lambda_1$. Using this we get $\mu_2 u_1 - \lambda_2 u_2 \in$

$l_1 \cap l_\infty$. A contradiction because they are disjoint. A similar argument verifies that $\lambda_3\mu_4 - \mu_3\lambda_4 = 0$. Taking $\{n_2, n_4, n_3, n_1\}$ as a basis we get the expressions of l_0, l_1, l_∞ that we want.
We define the following lines:

$$m_a := [< (a,0,0,1),(0,a,1,0) >], m_\infty = [< (0,0,0,1),(1,0,0,0) >], l_a = [< (a,0,0,1),(0,a,1,0) >]$$

for all $a \in \mathbb{F}_q$. It is easy to check that lines of the sets $\{l_a\}_{a\in\mathbb{F}_q} \cup \{l_\infty\}$ and $\{m_a\}_{a\in\mathbb{F}_q} \cup \{m_\infty\}$ are disjoint. Now we check that the set $R = \{l_a\}_{a\in\mathbb{F}_q} \cup \{l_\infty\}$ is a regulus. We know that the lines are disjoint. R has the property that each line l_a for all $a \in \mathbb{F}_q \cup \{\infty\}$ intersects with all m_b, we only have to calculate a determinant for each m_b and l_a. Suppose that there is a line S such that intersects with three lines of R. Using the last lemma we know that there are at most $q+1$ lines that intersects these three, and we know that this $q+1$ lines are the m_b. This implies that S is one of m_b. This implies S intersects all l_a. We have proved existence.
Now we will see that R is the unique regulus such that contains l_0, l_1, l_∞. Suppose that R' is a regulus that contains l_0, l_1, l_∞. Because of m_0, m_1, m_∞ intersect with this three lines of R' then they have to intersect with all lines of R'. But for the lemma 5.2 there are at most $q+1$ lines that intersects with m_0, m_1, m_∞ and we know that this $q+1$ lines are the lines of R. This implies $R = R'$.

□

Corollary 5.4. *The $q+1$ transversal lines of a regulus R form another regulus. We will denote it by $opp(R)$.*

Proof. Applying the same argument of the existence in the set $\{m_b\}_{b\in\mathbb{F}_q} \cup \{m_\infty\}$ we get that it is a regulus. □

5.2 Baer lines

In this subsection we will need to talk about field extensions to be able to define what is a Baer line. We will use the definition of regulus to define a Baer line and we will use some properties of them to study Baer lines.

Lemma 5.5. *Let L/K be a finite extension field of degree m. Let V a vector space over L of rank n. Then V is a vector space over K of rank nm.*

Proof. It is easy to check the axioms of a vector space over K using the axioms of V as a vector space over L. To check the multiplicity of the rank: let $\{e_1, ..., e_n\}$ be a basis of V as vector space over L and let $\{l_1, ..., l_m\}$ be a basis of the extension L/K. It is easy to check that $\{l_j e_i\}_{i,j}$ is a basis of V as a vector space over K. □

Let $q \geq 2$ a power of a prime. Consider the following map:

$$\psi: \text{ subspaces of } PG(2,q^2) \xleftrightarrow{\pi_1} \text{ subspaces of } V(3,q^2) \xrightarrow{i} \text{ subspaces of } V(6,q) \xleftrightarrow{\pi_2} \text{ subspaces of } PG(5,q)$$

where π_1, π_2 are correspondences between the projective subspaces and linear subspaces and i is the identification of the lemma 5.5 between subspaces of $V(3,q^2)$ and $V(6,q)$. Note that if W has dimension $n-1$ then $\psi(W)$ has dimension $2n-1$. When we will want to calculate this map, it will depend on the basis we will chose for the isomorphism between $V(6,q)$ and $V(3,q^2)$ seen as a vector field over $\mathbb{F}_q$. This fact is not important for the following definitions.

Definition 5.6. Let B a subset of a line of $PG(2, q^2)$ with $q+1$ points. For each $p \in B$ we have that $\psi(p)$ is a line of $PG(5, q)$. Let $R = \{\psi(p)|p \in B\}$. Since B has $q+1$ different points, R has $q+1$ disjoint lines. Since B is a subset of a line then all lines $\psi(p)$ for all $p \in B$ are in the same subspace V of PG(5,q) of dimension 3. We say B is a Baer line if and only if R is a regulus of V.

The Baer lines are very useful to find arcs in $PG(2, q)$ because if there are two Baer lines that share three points then they are the same. The idea is that in some cases it help us to know that some lines only share two points with a set and it is the main property of an arc.

Proposition 5.7. *Given* 3 *collinear points of* $PG(2, q^2)$ *then exists a unique Baer line that contain these three points.*

Proof. Let p_0, p_1, p_∞ be points of the line l of $PG(2, q^2)$. Then $\psi(p_0), \psi(p_1), \psi(p_\infty)$ define a unique regulus in $\psi(l)$. Suppose that we have the following subsets of l that complete p_0, p_1, p_∞ to a Baer line: $\{b_4, ..., b_{q+1}\}$ and $\{c_4, ..., c_{q+1}\}$. Then we have that $\{\psi(p_0), ..., \psi(b_{q+1})\}$ and $\{\psi(p_0), ..., \psi(c_{q+1})\}$ define the same regulus because they share $\psi(p_i)$ for $i = 0, 1, \infty$. Since ψ is one to one we get that the extensions are the same Baer line.
Now we prove existence. Let R be the regulus defined by $\psi(p_0), \psi(p_1), \psi(p_\infty)$. We have to check that all lines of R are the image of a point of l by ψ. Firstly we have to restrict ψ : points of $PG(1, q^2) \cong l \longrightarrow$ lines of $PG(3, q) \cong \psi(l)$. We can take a basis $\{v_1, v_2\}$ such that $p_0 = [(0, 1)]$, $p_1 = [(1, 1)]$, $p_\infty = [(1, 0)]$. Let ϵ be such that $\mathbb{F}_{q^2} = \mathbb{F}_q(\epsilon)$ and take a basis of $V(2, q^2) \cong V(4, q)$ $v_0, \epsilon v_0, \epsilon v_1, v_1$. Now we can calculate $\psi(p_0), \psi(p_1), \psi(p_\infty)$.

$$p_0 = [(0, 1)] \to \{\lambda(0, 1)|\lambda \in \mathbb{F}_{q^2}\} \to \{(\lambda_1 + \epsilon\lambda_2)(0, 1) = (\lambda_1 + \epsilon\lambda_2)v_1|\lambda_1, \lambda_2 \in \mathbb{F}_q\} \to$$

$$< (0, 0, 0, 1), (0, 0, 1, 0) >= l_0$$

This implies that $\psi(p_0) = l_0 =< (0, 0, 0, 1), (0, 0, 1, 0) >$. Doing the same we can find that $\psi(p_1) = l_1 =< (1, 0, 0, 1), (0, 1, 1, 0) >$ and $\psi(p_\infty) =< (1, 0, 0, 0), (0, 1, 0, 0) >$. Defining for each $a \in \mathbb{F}_q$ $l_a =< (a, 0, 0, 1), (0, a, 1, 0) >$ and using a previous proof we know that the regulus defined by l_0, l_1, l_∞ is $R = \{l_a\}_{a \in \mathbb{F}_q} \cup l_\infty$. We know that all points of $l \cong PG(1, q^2)$ have the form $[(a+\epsilon b, 1)]$ or $[(1, 0)]$ for $a, b \in \mathbb{F}_q$. If we check that $\psi([a, 1]) = l_a$ then we have $B = [(a, 1)]_{a \in \mathbb{F}_q} \cup \{p_\infty\}$ will be a Baer line.

$$[(a, 1)] \to \lambda(a, 1) \to \{\lambda_1(a, 0, 0, 1) + \lambda_2(0, a, 1, 0)\} \to < (a, 0, 0, 1), (0, a, 1, 0) >= l_a$$

□

The following proposition helps us to identify Baer lines:

Proposition 5.8. *Let* S *be a set of* $q+1$ *collinear points. Then* S *is a Baer line if and only if there exists a reference of the line containing* S *such that* S *has the form* $\{[(a, 1)]\}_{a \in \mathbb{F}_q} \cup \{[(1, 0)]\}$.

Proof. [⇒] As in the previous proof we can see this.
[⇐] As in the previous proof we can see that $R = \{\psi(p)|p \in S\}$ is a regulus. □

5.3 Linear sets

In this subsection we will study the linear sets. These sets will help us to find arcs in $PG(2, q^2)$ because in some cases they have the property that its intersection with a line is a Baer line.

Definition 5.9. Let U be a projective subspace of $PG(5,q)$. Ee define the linear set over U to be $B(U) = \{p \in PG(2,q^2) | \psi(p) \cap U \neq \emptyset\}$. It is a subset of points of $PG(2,q^2)$.

Proposition 5.10. *Let U be a projective subspace of $PG(5,q)$. Let l be a line of $PG(2,q^2)$ which intersects $B(U)$ in at least two points. We will call $V = \psi(l)$. If $r := U \cap V$ has dimension 1 then $l \cap B(U)$ is a Baer line.*

Proof. Since $l \cap B(U)$ has at least two points there are at least $q+1$ points $p \in l$ such that $\psi(p) \cap r \neq \emptyset$ because r is a line of $q+1$ points. Since the lines $\psi(p)$ are disjoint there are at most $q+1$ of them. This implies that $l \cap B(U)$ has exactly $q+1$ points. We have to check $R = \{\psi(p) | p \in l \cap B(U)\}$ is a regulus. R is a set of disjoint lines which lie in $V \cong PG(3,q)$. We know that given three points $p_1, p_2, p_3 \in l \cup B(U)$ we can extend $\psi(p_1), \psi(p_2), \psi(p_3)$ to a regulus R' in V such that the other lines have the form $\psi(p)$ for $p \in l$. We know that r is in $opp(R')$ because it contains $\psi(p_1), \psi(p_2), \psi(p_3)$. The lines of R are the only lines that are the images of points of l which have a non empty intersection with r. This implies $R = R'$. We have that R is a regulus. □

Proposition 5.11. *Let H be a non-degenerate hermitian curve of $PG(2,q^2)$ and let l be a line. If $H \cap l$ has at least two points then $H \cap l$ is a Baer line.*

Proof. Suppose that H is represented by the non-degenerate hermitian form $\varphi(x,y)$. We can restrict φ in l and it is non-degenerate because there are two points in the intersection and we can use Lemma 4.7. We know that there is a basis $\{v_1, v_2\}$ such that $\varphi_{|l}(x,y) = x_1 y_2^q + x_2 y_1^q$. This implies that the equation of H restricted in l is $x_1 x_2^q + x_2 x_1^q = 0$. In this basis every point of l has the form $[(a + b\epsilon, 1)]$ $a, b \in \mathbb{F}_q$ or $[(1,0)]$. Substituting this expression on the equation of H we get that all points of $H \cap l$ are $[((\epsilon + \frac{1}{2}\epsilon^q)b, 1)]$ for all $b \in \mathbb{F}_q$ and $[(1,0)]$. Taking the basis $\{(\epsilon + \frac{1}{2}\epsilon^q)v_1, v_2\}$ we have that the set $H \cap l$ is $[(a,1)]$ for all $a \in \mathbb{F}_q$ and $[(1,0)]$. Using Proposition 5.8 we get that $H \cap l$ is a Baer line. □

These propositions give us an idea how to try to construct an arc with the intersection between a linear set and a hermitian curve.
Let U be a projective subspace of $PG(5,q)$ of dimension 3. I would like to get an U such that for all lines l of $PG(2,q^2)$ we have that $\psi(l) \cap U$ has dimension 1. If this happens consider the linear set $B(U)$. We have that the set $S = B(U) \cap H$, where H is an hermitian curve, is very near to an arc. Let l be a line such that $S \cap l$ has at least three points. This three points define the same Baer line in $H \cap l$ and $B(U) \cap l$. Then $S \cap l$ has $q+1$ points. Then we have for each line the intersection with S has 1, 2 or $q+1$ points. Thus, we will want to avoid lines that intersect in $q+1$ points.

6. Scatared spaces

6.1 Spreads

In this section t, r will be integers such that $t, r \geq 2$.

Definition 6.1. A t-spread of a vector space V is a partition of $V-\{0\}$ by subspaces of rank t. Equivalently a $t-1$-spread of PG(V) is a partition of the points of $PG(V)$ by projective subspaces of dimension $t-1$.

We want to construct a spread. Take any $\mathbb{F}_q$-vector space isomorphism from $\mathbb{F}_{q^t} \longrightarrow \mathbb{F}_q^t$. We can extent this to a isomorphism φ from $\mathbb{F}_{q^t}^r \longrightarrow \mathbb{F}_q^{rt}$ of $\mathbb{F}_q$-vector spaces. For each non-zero vector $v \in V(r, q^t)$ define $S_v = \{\varphi(\lambda v) | \lambda \in \mathbb{F}_{q^t}\}$. It is easy to see that the set $D_{r,t,q} := \{S_v | v \in V(r, q^t)\}$ is a spread. We will call that S_1, S_2 spreads are equivalent if and only if there exists an automorphism σ of $\mathbb{F}_q^{rt}$ such that $S_1 = S_2^\sigma$. We will call S a Desarguesian spread if it is equivalent to $D_{r,t,q}$ for some r, t, q. But in practice we will suppose that all Desarguesian spreads have the form $D_{r,t,q}$ because they have the same properties under isomorphism. Note that $\mathbb{F}_{q^t}^r = V(r, q^t)$ and $\mathbb{F}_q^{rt} = V(rt, q)$.

Now we will define a map between the subspaces of $V(r, q^t)$ and subspaces of $V(rt, q)$ that will help us to work with scattered spaces and Desarguesian spreads.

Definition 6.2. Let φ be a $\mathbb{F}_q$-vector spaces isomorphism between $\mathbb{F}_{q^t}^r$ and $\mathbb{F}_q^{rt}$ defined on the same way in Desarguesian spreads. Then we define:

$$\psi : \text{ subspaces of } V(r, q^t) \longrightarrow \text{ subspaces of } V(rt, q)$$

such that $\psi(H) = \varphi(H)$ where H subspace of $V(r, q^t)$.

Note that for each Desarguesian spread we can associate a ψ and we can define the spread in the following way $S = \{\psi(p) | p \in PG(r-1, q^t)\}$. An important thing is that the ψ defined in the last section is one of these and defines a Desarguesian spread.

Definition 6.3. Let D be a spread of $V(n, q)$. Let W be a subspace of $V(n, q)$. We will say that W is scattered with respect to D if W intersects with all subspaces of D in at most rank 1. Equivalently we will say that subspace W of $PG(n, q)$ is scattered with respect to a spread D of $PG(n, q)$ if W intersects to all subspaces of D in at most one point.

Scattered subspaces were introduced in [4]. An example of a scattered space with respect to D, a 1-spread of $PG(3, q)$, is a line that it is not in the spread. This line intersects with $q+1$ lines of D in one point and is skew to the others. Because of a plane of $PG(3, q)$ has q^2+q+1 points and D has q^2+1 lines then we have that the plane contain exactly one line of the spread. This implies that the planes won't be scattered. This implies that won't exist scattered planes of $PG(3, q)$ with respect to D. A scattered space of highest possible dimension is called maximum scattered space. In this example every line not contained in D is a maximum scattered space with respect to D.

The next definition is an extension of the linear sets in higher dimensions:

Definition 6.4. Let ψ be a map as in the definition 6.2. Let U be a subspace of $PG(rt-1, q)$. We define the linear set of the subspace U in the following way:

$$B(U) := \{p \in PG(r-1, q^t) | \psi(p) \cap U \neq \emptyset\}$$

The linear set associated to a scattered space has interesting properties.

Lemma 6.5. *Suppose that we have a Desarguesian spread D in $PG(rt-1,q)$ defined by ψ. Let U be a scattered subspace with respect to D. Then we have a bijection between $B(U)$ and U defined by:*

$$T : B(U) \longrightarrow U$$

where $T(p) = \psi(P) \cap U$.

Proof. Firstly we have to check that T is well defined. Let $p \in B(U)$, because $\psi(p) \cap U \neq \emptyset$ and using that U is scattered we get that $\psi(p) \cap U$ has exactly one point.
Since $\psi(p)$ are disjoint for distinct p, we have that T is injective. Now we check that T is surjective: let $q = [u] \in U$, then it is easy to see that $T([\varphi^{-1}(u)] = q$. □

6.2 Scattered spaces with respect to Desarguesian spreads

In this subsection we will see bounds on the dimension and the existence in some dimensions of scattered spaces with respect to Desarguesian spreads.

Proposition 6.6. *Suppose that rt is even. Let $W_{\frac{rt}{2}}$ a subspace of rank $\frac{rt}{2}$ of $V(rt,q)$ such that is scattered respect a Deserguesian t-spread S of $V(rt,q)$. Then $B(W_{\frac{rt}{2}})$ will be an 2-intersection set with respect to hyperplanes with intersection numbers $\Theta_{\frac{rt}{2}-t-1}(q), \Theta_{\frac{rt}{2}-t}(q)$.*

Proof. Let m an integer such that $2m = rt$. For $i = 1, ..., m$, define h_i as the number of hyperplanes H of $PG(r-1,q^t)$ such that $\psi(H)$ intersects W_m in a subspace of rank i. Using Green's formula we can deduce that W_m intersects with $\psi(H)$ in a subspace of rank at least $m-t$. Since W_m is scattered, we have that $\psi(H) \cup W_m$ has rank at most $rt-2t$.
Now we will deduce three equations that help us in the next step of the proof:
The first equation we will count all the hyperplanes of $PG(r-1,q^t)$ in two different ways: It is clear that it is $\sum_{i=m-t}^{rt-2t} h_i$. In other way we know for duality of $PG(r-1,q^t)$ that the number of hyperplanes is the same of the points: $\Theta_{r-1}(q^t)$. Using this we deduce the following equation:

$$\sum_{i=m-t}^{rt-2t} h_i = \Theta_{r-1}(q^t) \tag{4}$$

We can get the second equation counting in two different ways the pairs (P, H) where H is an hyperplane of $PG(r-1,q^t)$ and $P \in B(U)$ such that $P \in H$. Because of W_m is scattered we have a bijection between $B(W_m)$ and W_m. This implies that for each hyperplane H there are the same points to $B(W_m) \cap H$ and $W_m \cap \psi(H)$. Using this and counting the pairs fixing the hyperplane we have that there are $\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q) h_i$. Because of the bijection we know that there are $\Theta_{m-1}(q)$ points in $B(U)$. In $PG(r-1,q^t)$ we know that the hyperplanes through a point is a hyperplane in the dual space. This implies that there are $\Theta_{m-1}(q)\Theta_{r-2}(q^t)$. Then we get the second equation:

$$\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q) h_i = \Theta_{m-1}(q)\Theta_{r-2}(q^t) \tag{5}$$

To deduce the third equation we will count the triples (P, Q, H) where H is an hyperplane of $PG(r-1, q^t)$ and P, Q two different points of $B(W_m)$ such that $P, Q \in H$. Doing a similar calculation as in the last equation we have that the number of triples is $\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q)(\Theta_{i-1}(q)-1)h_i$. We can choose $\Theta_{m-1}(q)(\Theta_{m-1}(q)-1)$ pairs of different points P, Q of $B(W_m)$. Then we need that the hyperplane H contains P, Q and this happen if and only if H contain the line joining P, Q. The set of hyperplanes that contain a fixed line form a variety of dimension $r-3$ in the dual space. This implies that we have $\Theta_{m-1}(q)(\Theta_{m-1}(q)-1)\Theta_{r-3}(q^t)$. Using this we found the last equation:

$$\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q)(\Theta_{i-1}(q)-1)h_i = \Theta_{m-1}(q)(\Theta_{m-1}(q)-1)\Theta_{r-3}(q^t) \tag{6}$$

Consider the following expression:

$$\sum_{i=m-t}^{rt-2t} (\Theta_{i-1}(q) - \Theta_{m-t-1}(q))(\Theta_{i-1}(q) - \Theta_{m-t}(q))h_i$$

Expanding the products and extracting the common factors we get:

$$\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q)(\Theta_{i-1}(q)-1)h_i +$$

$$-(\Theta_{m-t-1}(q) + \Theta_{m-t}(q) - 1)(\sum_{i=m-t}^{rt-2t} \Theta_{i-1}(q)h_i) + \Theta_{m-t-1}(q)\Theta_{m-t}(q)(\sum_{i=m-t}^{rt-2t} h_i)$$

Using the equations (4), (5) and (6) on the above expression we get:

$$\Theta_{m-1}(q)(\Theta_{m-1}(q)-1)\Theta_{r-3}(q^t) +$$

$$-(\Theta_{m-t-1}(q) + \Theta_{m-t}(q) - 1)\Theta_{m-1}(q)\Theta_{r-2}(q^t) + \Theta_{m-t-1}(q)\Theta_{m-t}(q)\Theta_{r-1}(q^t)$$

We know the value of $\Theta_i(q)$ for all integer i and all prime power q. Substituting it we get that the expression is equal to 0. This implies:

$$\sum_{i=m-t}^{rt-2t} (\Theta_{i-1}(q) - \Theta_{m-t-1}(q))(\Theta_{i-1}(q) - \Theta_{m-t}(q))h_i = 0$$

This says us that $h_i = 0$ for $i \neq m-t, m-t+1$. This implies that $W_m \cap \psi(H)$ has rank $m-t$ or $m-t+1$ where H is an hyperplane of $PG(r-1, q^t)$. Since W_m is scattered and we have a bijection between W_m and $B(W_m)$ then we have that $B(W_m) \cap H$ has $\Theta_{m-t}(q)$ or $\Theta_{m-t+1}(q)$ points. This is what we have to prove. □

The following proposition says us that the every scattered space with respect to $(t-1)$-spread of $PG(rt-1, q)$ has at most dimension $\frac{rt}{2} - 1$. We will use this in the future for classify the linear sets in $PG(2, q^2)$

Proposition 6.7. *The dimension of a maximum scattered space with respect to $(t-1)$-spread of $PG(rt-1, q)$ is at most $\frac{rt}{2} - 1$.*

Proof. The claim is equivalent to claiming that every scattered space with respect to t-spread of $V(rt, q)$ has at most rank $\frac{rt}{2}$. Let W_m a scattered subspace respect to t-spread of $V(rt, q)$. Suppose that W_m has rank m. Consider the following expression:

$$(q^t - 1)(q - 1)^2 \sum_{i=m-t}^{rt-2t} (\Theta_{i-1}(q) - \Theta_{m-t-1}(q))(\Theta_{i-1}(q) - \Theta_{m-t}(q))h_i \tag{7}$$

We can use the equations (4),(5) and (6) of the proposition 6.6 because only require that W_m will be scattered. Then we get that the expression 7 is equal to:

$$(q^m-1)(q^m-q)(q^{rt-2t}-1)-(q^{m-t}+q^{m-t+1}-q-1)(q^m-1)(q^{rt-t}-1)+(q^{m-t}-1)(q^{m-t+1}-1)(q^{rt}-1) =$$
$$(q^{rt-2t+1} + q^{2m-t+1} + q^{2m-t} + q^{rt}) - (q^{rt-t+1} + q^{2m-2t+1} + q^{2m} + q^{rt-t}) =$$
$$(q^{2m} - q^{rt})(q^{1-t} - q^{1-2t} + q^{-t} - 1)$$

Expression 7 has all non-negative terms which implies that:

$$(q^{2m} - q^{rt})(q^{1-t} - q^{1-2t} + q^{-t} - 1) \geq 0$$

Suppose that $m > \frac{rt}{2}$. Then we have that $q^{2m} - q^{rt} > 0$ and since $q^{1-t} - q^{1-2t} + q^{-t} - 1 < 0$ for $q, t \geq 2$ this implies that:

$$(q^{2m} - q^{rt})(q^{1-t} - q^{1-2t} + q^{-t} - 1) < 0.$$

This is a contradiction, which implies that $m \leq \frac{rt}{2}$. □

The following lemma give us a lower bound of the dimension of a maximum scattered space with respect to $(t-1)$-spread. Note that the spread doesn't have to be Desarguesian.

Lemma 6.8. *Let S be a $(t-1)$-spread of $PG(rt-1, q)$ and let T be an m-dimensional scattered space with respect to S. If $m < \frac{rt-t}{2}$ then we have that T is contained in $(m+1)$-dimensional scattered space with respect to S. This implies that the dimension of a maximum scattered space with respect to S is at least $\frac{rt-t}{2}$.*

Proof. Let S be a t-spread in $V(rt, q)$ and let $T =< w_0, ..., w_m >$ be a scattered with respect to S of rank $m+1$. Take $w_{m+1} \in V(rt, q)$ such that $w_{m+1} \notin T$. We have to check that:

$$< T, w_{m+1} > \text{ is not scattered} \Leftrightarrow w_{m+1} \in \cup_{Q \in S | Q \cap T \neq \{0\}} < Q, T >$$

Suppose that $< T, w_{m+1} >$ is not scattered. Then we have that exists $Q \in S$ such that $< T, w_{m+1} > \cap Q$ has at least rank 2. Suppose that $< v_1, v_2 > \subset < T, w_{m+1} > \cap Q$ and v_1, v_2 linearly independents. Then we have:

$$\begin{cases} v_1 = u_1 + \lambda_1 w_{m+1} \\ v_2 = u_2 + \lambda_2 w_{m+1} \end{cases}$$

Where $u_1, u_2 \in T$. Because T is scattered with respect to S it is impossible to have $\lambda_1 = \lambda_2 = 0$. Suppose $\lambda_1 \neq 0$. Then we have that $w_{m+1} = \frac{1}{\lambda_1} v_1 - \frac{1}{\lambda_1} u_1 \in < Q, T >$. Using a linear combination of the equation of v_1 and v_2 we can find a vector of $Q \cap T$. Now we have to prove the other implication. Suppose that $w_{m+1} \in < Q, T >$ for some $Q \in S$ such that $Q \cap T \neq \{0\}$. We will see that $Q \cap < T, w_{m+1} >$ has rank 2. Take a non trivial $w \in Q \cap T$. We know that $w_{m+1} \in < Q, T >$ this implies that $w_{m+1} = u + v$ where $u \in Q$ and $v \in T$. Then we have that $u \in Q \cap < T, w_{m+1} >$. It is clear that u, w are l.i. and

$w, u \in Q \cap < T, w_{m+1} >$.
This tells us that T is contained in a space of rank $m+2$ if $w_{m+1} \notin \cup_{Q \in S | Q \cap T \neq \{0\}} < Q, T >$. Firstly we have to count the number of non zero vectors of $\cup_{Q \in S | Q \cap T \neq \{0\}} < Q, T >$. Take $Q \in S$ such that $Q \cap T \neq \{0\}$. This implies that $Q \cap T$ has rank 1 because T is scattered. The rank of $< Q, T >$ is $t+m$ using Grassmann. This implies that there are $q^{t+m} - q^m$ vectors in $< Q, T > -T$. Since T is scattered, there exists $Q \in S$ such that $Q \cap H \neq \{0\}$ for each point of T. This implies that there are $\Theta_m(q) = q^m + ... + 1$ Q of this type. Then in $\cup_{Q \in S | Q \cap T \neq \{0\}} < Q, T >$ there are $(q^{m+t} - q^m)(q^m + ... + q + 1) + q^{m+1} - 1$ non null vectors. But we need that this number will be smaller than the number of non null vectors in $V(rt, q)$ that it is $q^{rt} - 1$. We need that:

$$q^{rt} > (q^{m+t} - q^m)(q^m + ... + q + 1) + q^{m+1}$$

Supposing $m < \frac{rt-t}{2}$ suffices. □

The following proposition proves the existence of maximum scattered spaces with respect to Desarguesian 1-spreads of $PG(2r-1, q)$. This is all we need because in this thesis we work always with a line spread.

Proposition 6.9. *Let S be a Desarguesian 1-spread of $PG(2r-1, q)$. Then the dimension of maximum scattered space with respect to S will be $r-1$.*

Proof. This is an immediate consequence of Lemma 6.8 and Proposition 6.7. □

7. Trying to construct an arc

7.1 Programming in GAP

In this section we will see how I have found examples of linear sets with the help of the computer to try construct an arc. I use GAP to program the calculations. The programs are included in the annex.

Firstly, for the calculations we choose $\epsilon \in \mathbb{F}_{q^2}$ such that $\mathbb{F}_{q^2} = \mathbb{F}_q(\epsilon)$. Since we have an extension of degree 2, $\epsilon^2 = a\epsilon + b$ for some $a, b \in \mathbb{F}_q$. We have to calculate $\psi : PG(2, q^2) \longrightarrow$ lines of $PG(5, q)$. Let $[v]$ be a point of $PG(2, q^2)$:

$$[v] \longrightarrow \{\lambda v | \lambda \in \mathbb{F}_{q^2}\} \longrightarrow \{(\lambda_1 + \epsilon\lambda_2)v | \lambda_1, \lambda_2 \in \mathbb{F}_q\} \longrightarrow [< v, \epsilon v >]$$

where $[< v, \epsilon v >]$ is a line of $PG(5, q)$. Take a basis v_1, v_2, v_3 of $V(3, q^2)$ then we can construct a basis of $V(6, q)$ taking $v_1, v_2, v_3, \epsilon v_1, \epsilon v_2, \epsilon v_3$. Let $v = xv_1 + yv_2 + zv_3$ where $x, y, z \in \mathbb{F}_{q^2}$ and $x = x_1 + \epsilon x_2, y = y_1 + \epsilon y_2, z = z_1 + \epsilon z_2$ where $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{F}_q$. Now we have to found the expression of $v, \epsilon v$ on the basis of $V(6, q)$:

$$v = xv_1 + yv_2 + zv_3 = (x_1 + \epsilon x_2)v_1 + (y_1 + \epsilon y_2)v_2 + (z_1 + \epsilon z_2)v_3 = x_1v_1 + y_1v_2 + z_1v_3 + x_2\epsilon v_1 + y_2\epsilon v_2 + z_2\epsilon v_3$$

$$\epsilon v = \epsilon x v_1 + \epsilon y v_2 + \epsilon z v_3 = (\epsilon x_1 + \epsilon^2 x_2)v_1 + (\epsilon y_1 + \epsilon^2 y_2)v_2 + (\epsilon z_1 + \epsilon^2 z_2)v_3 =$$

$$= (\epsilon x_1 + (a\epsilon + b)x_2)v_1 + (\epsilon y_1 + (a\epsilon + b)y_2)v_2 + (\epsilon z_1 + (a\epsilon + b)z_2)v_3$$

$$= x_2 b v_1 + y_2 b v_2 + z_2 b v_3 + (x_1 + x_2 a)\epsilon v_1 + (y_1 + y_2 a)\epsilon v_2 + (z_1 + z_2 a)\epsilon v_3$$

Choosing $v_i = e_i$ we have that ψ sends $[(x, y, z)]$ to $[< (x_1, y_1, z_1, x_2, y_2, z_2), (x_2 b, y_2 b, z_2 b, x_1 + x_2 a, y_1 + y_2 a, z_1 + z_2 a) >]$. Now the problem is given a $x \in \mathbb{F}_{q^2}$ found efficiently $x_1, x_2 \in \mathbb{F}_q$ such that $x = x_1 + \epsilon x_2$. To solve it at the start of the code I build an ordered vector of tuples where each tuple has the form (x, x_1, x_2). It is easy to calculate taking each $x_1, x_2 \in \mathbb{F}_q$ and using that each $x \in \mathbb{F}_{q^2}$ has a unique expression of this type. Since the vector is ordered it is efficient to ask for any $x \in \mathbb{F}_{q^2}$. To calculate a random linear set of rank n, firstly we choose n random vectors of $V(6, q)$ and then for each point $p \in PG(2, q^2)$ asks if $u_1, ..., u_n, \psi(p)$ has maximum rank. Since we choose a random linear set we can fix the hermitian curve $xy^q + yx^q + z^{q+1} = 0$ of $PG(2, q^2)$. Then we will be interested to know the secant distribution of the intersection of these sets. The secant distribution of a set S is the sequence of numbers $\{T_i\}_{i \geq 0}$ where T_i is the number of lines which intersect S in i points. If we have $T_i = 0$ for all $i \geq 3$ then the set will be an arc.

7.2 Intersection between a linear set and a hermitian curve

When we intersect a linear set and a hermitian curve with gap we get the following results. Let S be the intersection:
For $q = 3$ we found 4 distinct tangent distributions: Table 1. For $q = 7$ we found 4 distinct tangent distributions: Table 2.

Proposition 7.1. *Let U be a projective subspace of $PG(5, q)$. Let L be a line of $PG(2, q^2)$. Let H be a hermitian curve of $PG(2, q^2)$. If $dim(U \cap \psi(L)) \geq 2$ and L is not tangent to H then $L \cap H \cap B(U)$ is a Baer line.*

$\|S\|$	T_0	T_1	T_2	T_4
13	18	30	36	7
4	54	36	0	1
10	27	34	27	3
16	15	16	48	12

Table 1: Tangent distribution $S = H \cap B(U)$, $q = 3$

$\|S\|$	T_0	T_1	T_2	T_8
57	882	378	1176	15
50	1050	338	1057	6
8	2058	392	0	1
64	763	320	1344	24

Table 2: Tangent distribution $S = H \cap B(U)$, $q = 7$

Proof. Firstly we will see that $L \subset B(U)$. Take a point $p \in L$ then $\psi(p) \subset \psi(L)$. We know that $\psi(L)$ has dimension 3 and $\psi(L) \cap U$ has dimension 2. Using this and Green's formula we get that $dim(\psi(p) \cap U) \geq 0$ which implies that $\psi(p) \cap U \neq \emptyset$. By the definition of $B(U)$ we have $p \in B(U)$.
We have $L \subset B(U) \Rightarrow L \cap B(U) \cap H = L \cap H$ and it is clear that it is a Baer line since there are at least two points. □

Then next proposition gives a structure to the linear sets of $B(U)$ when U has dimension 3.

Proposition 7.2. *Let U be a projective subspace of $PG(5, q)$ of dimension 3. Then we have two cases for $B(U)$:*

- *There exists only one $P \in PG(2, q^2)$ such that $\psi(P) \subset U$ then the set of lines contained in $B(U)$ is a bear line in $PG(2, q^2)^*$.*
- *There exists at least two $P_1, P_2 \in PG(2, q^2)$ such that $\psi(P_1), \psi(P_2) \subset U$. Let L be the line defined by P_1, P_2. Then we have $B(U) = L$.*

Proof. There always exists a $P \in PG(2, q^2)$ such that $\psi(P) \subset U$ since Proposition 6.7 implies that U can't be scattered with respect to $D_{3,2,q}$ since U has rank 4.

If it has two points P_1, P_2 such that $\psi(P_1), \psi(P_2) \subset U$ then $\psi(P_1) + \psi(P_2) \subseteq U$, which implies that $\psi(L) \subseteq U$ and they have the same dimension. This implies that $\psi(L) = U$ and since distinct lines have disjoint images we get $L = B(U)$.

Suppose that there exists only one point $P = [u] \in PG(2, q^2)$ such that $\psi(P) \subset U$. Then we can express $U =< u, \epsilon u, v_1, v_2 >$ such that $\{u, v_1, v_2\}$ is a basis of $V(3, q^2)$. We have to check this, let $\lambda_i \in \mathbb{F}_{q^2}$:

$$\lambda_0 u + \lambda_1 v_1 + \lambda_2 v_2 = 0 \Rightarrow \lambda_{01} u + \lambda_{02} \epsilon u + \lambda_{11} v_1 + \lambda_{12} \epsilon v_1 + \lambda_{21} v_2 + \lambda_{22} \epsilon v_2 = 0 \Rightarrow$$

$$\lambda_{01} u + \lambda_{02} \epsilon u + \lambda_{11} v_1 + \lambda_{21} v_2 = -\lambda_{12} \epsilon v_1 - \lambda_{22} \epsilon v_2$$

Where $\lambda_{ij} \in \mathbb{F}_q$. If we have $\lambda_{01}u+\lambda_{02}\epsilon u+\lambda_{11}v_1+\lambda_{21}v_2 = -\lambda_{12}\epsilon v_1-\lambda_{22}\epsilon v_2 = 0$ this implies that $\lambda_{ij} = 0$ because $\{v, \epsilon v, v_1, v_2\}$ and $\{\epsilon v_1, \epsilon v_2\}$ are linearly independent in $V(6, q)$. And we have that $\{u, v_1, v_2\}$ are linearly independent in $V(3, q^2)$.
Suppose that $\lambda_{01}u+\lambda_{02}\epsilon u+\lambda_{11}v_1+\lambda_{21}v_2 = -\lambda_{12}\epsilon v_1-\lambda_{22}\epsilon v_2 \neq 0$. Let $Q = [-\lambda_{12}v_1-\lambda_{22}v_2]$ be a point of $PG(2, q^2)$. Then we have $\psi(Q) \subset U$ since $-\lambda_{12}v_1 - \lambda_{22}v_2 \in U$ and $\epsilon(-\lambda_{12}v_1 - \lambda_{22}v_2) = -\lambda_{12}\epsilon v_1 - \lambda_{22}\epsilon v_2 = \lambda_{01}u + \lambda_{02}\epsilon u + \lambda_{11}v_1 + \lambda_{21}v_2 \in U$. This implies that $Q = P$ since we supposed that P is the unique point such that $\psi(P) \subset U$. This implies the following equality: $\lambda_{12}v_1 + \lambda_{22}v_2 = \mu u = \mu_1 u + \mu_2 \epsilon u$. All coefficients are in $\mathbb{F}_q$ and these vectors are linearly independent in $V(6, q)$. This implies that all coefficients have to be 0. This is a contradiction because it is a representation of a point.

We define the following set of lines:

$$\mathcal{A} = \{L \in PG(2, q^2)^* | P \in L \text{ and } dim(\psi(L) \cap U) = 2\}$$

We want to prove that $\cup_{L\in\mathcal{A}} L = B(U)$. Suppose that L is a line of $PG(2, q^2)$ such that contains P. Since $P \in L$ we know that $\psi(L) \cap U$ has at least dimension 1. Suppose that $\psi(L) \cap U$ has dimension 3. Then $\psi(L) \subset U$ and this is the case one. We have proved that $\psi(L) \cap U$ has dimension 1 or 2. If we have $dim(\psi(L) \cap U) = 2$ then L will be a subset of $B(U)$. If $dim(\psi(L) \cap U) = 1$ then $\psi(L) \cap U = \psi(P)$ and this implies that $L \cap B(U) = \{P\}$. Firstly we will prove the following inclusion: $\cup_{L\in\mathcal{A}} L \subset B(U)$. It is clear because for each $L \in \mathcal{A}$ has the property that $\psi(L) \cap U$ has dimension 2 and this implies that $L \subset B(U)$.

Now we have to prove the other inclusion. Let $Q \in B(U)$. If $Q = P$ then it is clear that $Q \in \cup_{L\in\mathcal{A}}$. Suppose that $Q \neq P$. Then exists a line L such that $P, Q \in L$. This implies that $\psi(L) \cap U$ has dimension 2. Now we have that $L \in \mathcal{A}$. We have proved the equality.
Now we want to prove that the set $\mathcal{A}$ is a bear line in $PG(2, q^2)^*$. Firstly we will see the following equality: $\mathcal{A} = \{L_a\}_{a\in\mathbb{F}_q} \cup \{L_\infty\}$ where $L_a =< u, v_1 + av_2 >$ and $L_\infty =< u, v_2 >$. We know that $U =< u, \epsilon u, v_1, v_2 >$ where $\{u, v_1, v_2\}$ is a basis of $V(3, q^2)$. Let L be a line of the set $\mathcal{A}$ then $L =< u, s >$ and $\psi(L) =< u, \epsilon u, s, \epsilon s >$. To impose that $\psi(L) \cap U$ will have 3 we have to impose that $\psi(L) + U$ has at most rank 5. This is equivalent to the existence of a non-trivial linear combination with coefficients in $V(6, q)$ of the vectors $s, \epsilon s, u, \epsilon u, v_1, v_2$:

$$\lambda_1 s + \lambda_2 \epsilon s + \lambda_3 u + \lambda_4 \epsilon u + \lambda_5 v_1 + \lambda_6 v_2 = 0 \Rightarrow$$

$$(\lambda_1 + \epsilon\lambda_2)s = \lambda_1 s + \lambda_2 \epsilon s = -\lambda_3 u - \lambda_4 \epsilon u - \lambda_5 v_1 - \lambda_6 v_2$$

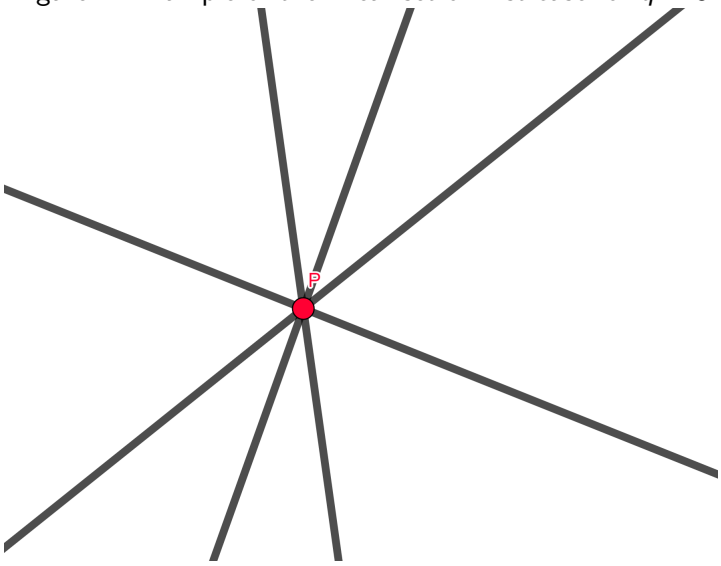
Since $u, \epsilon u, s, \epsilon s$ are linearly independent in $V(6, q)$ we have that $(\lambda_5, \lambda_6) \neq (0, 0)$. Using the last equality we get:

$$L =< u, s >=< u, (\lambda_1 + \epsilon\lambda_2)s >=< u, -\lambda_3 u - \lambda_4 \epsilon u - \lambda_5 v_1 - \lambda_6 v_2 >=$$

$$=< u, \lambda_5 v_1 + \lambda_6 v_2 >$$

It is clear that L is one of the L_a with $a \in \mathbb{F}_q$ or L_∞. This proves one inclusion and the other is trivial. Now we only have to see that the set $\{L_a\}_{a\in\mathbb{F}_q} \cup \{L_\infty\}$ is a bear line in $PG(2, q^2)^*$. Take $\{w_0, w_1, w_2\}$ the basis of $V(3, q^2)^*$ associated with $\{u, v_1, v_2\}$. We will take the basis $w_1, -w_2$ of P^* the line of $PG(2, q^2)^*$ associated to P. Then $L_a = [aw_1 - w_2] = [(a, 1)]$ and $L_\infty = [w_1] = [(1, 0)]$, which implies that this set is a bear line. □

Figure 1: Example of the linear set of first case for $q = 3$



7.3 More about hermitian curves

The objective of this section is prove that in $PG(2, q^2)$ the set of lines L such that L is incident with fix P and is tangent to a fix hermitian curve then this set of lines is a bear line on the dual projective space.

Lemma 7.3. *Let H a non-degenerate hermitian surface of $PG(n, q^2)$ represented by h. Let $PG(n, q^2)^*$ the dual projective space of $PG(n, q^2)$. Then for each $[w] \in PG(n, q^2)^*$ exists a unique $[x] \in PG(n, q^2)$ such that $[w] = [h(., x)]$.*

Proof. Existence: Let $v_1, ..., v_{n+1}$ a basis of $V(n+1, q^2)$ so that the hermitian form is $h(x, y) = x_1 y_2^q + x_2 y_1^q + ... + x_n y_{n+1} + x_{n+1} y_n^q$ (suppose that n is odd, if n is pair is the same procedure). Take $w_1, ...w_{n+1}$ the dual basis associate to the basis $v_1, ..., v_{n+1}$. Let $w = \lambda_1 w_1 + ... + \lambda_{n+1} w_{n+1} \in V(n+1, q^2)^*$ we have to found a vector $x = x_1 v_1 + ... + x_{n+1} v_{n+1} \in V(n+1, q^2)$ such that for all vector $y = y_1 v_1 + ... + y_{n+1} \in V(n+1, q^2)$ we have $w(y) = y_1 \lambda_1 + ... + y_{n+1} \lambda_{n+1} = y_1 x_2^q + ... + y_{n+1} x_n^q$. Because of an automorfism on a field is bijective we can take $x_1, ..., x_n$ so that the equality will be true for each $y \in V(n, q^2)$.
It is clear that exists a unique $[x] \in PG(n, q^2)$ because in the equation we can take $y_i = 0$ for $i \neq j$ and $y_j = 1$. □

We can see that there are there are a correspondence between $V(n, q^2)$ and $V(n, q^2)^*$ sending x to $h(., x)$.

The following proposition will help us to identify the hyper-planes such that are tangent to an hermitian curve. The idea is the same as in dimension 2.

Proposition 7.4. *Let $W \in PG(n, q^2)^*$ and let H be a non-degenerate hermitian curve of $PG(n, q^2)$. Then W is tangent to H if and only if $W = [h(., y)]$ for some $[y] \in H$.*

Proof. Firstly we see that if $[y] \in H$ then we have that $[h(., y)]$ is tangent to H. Suppose that exists a point $[x] \in H$ such that $h(x, y) = 0$. Then this implies that all points of $L =< x, y >$ will be in H. It means that H is degenerate, which is a contradiction.

Finally we see that if $[h(.,y)]$ is tangent to H then we have that $[y] \in H$. If we see that there is only one hyperplane tangent to H through $[y]$ we will have finished. Suppose that there is a hyperplane M tangent to $[y]$ that is not $[h(.,y)]$. Then we have that there exists $[x] \in M - H$ such that $h(x,y) \neq 0$. Doing a similar proof for dimension 2 we know that the line $L =< x, y >$ has $q+1$ points in common with H. This implies that M is not a tangent because it contains L, a contradiction. We have proved that $[h(.,y)]$ is the unique hyperplane tangent to H through $[y]$. □

The following theorem is the main result of this subsection since the objective of this subsection will be a corollary of this. But firstly we observe that we can extend easily the definition of hermitian curve to the dual space and we have the same properties since $V(n,q^2)^* \equiv V(n,q^2)$.

Theorem 7.5. *Let H be a non-degenerate hermitian curve of $PG(n,q^2)$. Define:*

$$H^* = \{W \in PG(n,q^2)^* | W \text{ is tangent to } H\}$$

is a subset of the dual space. Then H^* is a non-degenerate hermitian curve of $PG(n,q^2)^*$.

Proof. Define $\beta : V(n+1,q^2)^* \longrightarrow \mathbb{F}_{q^2}$ on the following way:

$$\beta(h(.,x),h(.,y)) = h(y,x)$$

It is clear that β is a non-degenerate hermitian form on the dual because h is a non-degenerate hermitian form. Let B the hermitian curve associate to b on the dual projective space. Because of the definition we have:

$$[h(.,x)] \in B \Leftrightarrow [x] \in H \Leftrightarrow [h(.,x)] \in H^*$$

□

The following corollary is an immediately consequence of the theorem.

Corollary 7.6. *Let H be a non-degenerate hermitian curve of $PG(2,q^2)$. Take a point $p \in PG(2,q^2)$. Then if the set of lines*

$$B = \{L \in PG(2,q^2) | p \in L \text{ and } L \text{ is tangent to } H\}$$

has at least two lines then it is a bear line in $PG(2,q^2)^*$.

Proof. We know that the set of lines through a point in the dual space is a line. Using Theorem 7.5 we know that the set of lines tangents to H is a non-degenerate hermitian curve. B is the intersection between these last two sets. If it has at least two lines it will be a bear line. □

The following proposition will help us to understand why we don't get an arc.

Proposition 7.7. *Let H be a non-degenerate hermitian curve represented by h. Let A be a set of points of H. We define the following set of $PG(2,q^2)^*$:*

$$B = \{L \in PG(2,q^2)^* | L \text{ is tangent to } H \text{ through a point in } A\}$$

B is the set of tangents of H through a point in A. Then we have that A is a bear line in $PG(2,q^2)$ if and only if B is a bear line in $PG(2,q^2)^*$.

Proof. Using the above propositions it is clear that we can express B in the following form:

$$B = \{[h(.,v)] \in PG(2,q^2)^* | [v] \in A\}$$

Firstly suppose that A is a bear line. This means that exists $v_1, v_2 \in V(3,q^2)$ such that:

$$A = \{[av_1 + v_2] | a \in \mathbb{F}_q\} \cup \{[v_1]\}$$

Take the elements $w_1 = h(.,v_1)$ and $w_2 = h(.,v_2)$ of $V(3,q^2)^*$. We know that the elements of B are $h(.,v)$ for each $[v]$ in A.

$$h(.,v) = h(.,av_1 + v_2) = ah(.,v_1) + h(.,v_2) = aw_1 + w_2$$

We have used that $a^q = a$ because $a \in \mathbb{F}_q$. This says us that $B = \{[(a,1)]\}_{a \in \mathbb{F}_q} \cup \{[(1,0)]\}$ in the basis w_1, w_2. It is clear that B is a bear line.
Now suppose that B is bear line in $PG(2,q^2)^*$. This implies that exists $w_1, w_2 \in V(3,q^2)^*$ such that:

$$B = \{[aw_1 + w_2] | a \in \mathbb{F}_q\} \cup \{[w_1]\}$$

Using Proposition 7.4 we know that $w_i = h(.,v_i)$ for some $v_i \in V(3,q^2)^*$

$$aw_1 + w_2 = ah(.,v_1) + h(.,v_2) = h(.,av_1 + v_2).$$

This implies that the points of A are $[av_1 + v_2]$ for $a \in \mathbb{F}_q$ and v_1, since the lines of B are tangent to these points. This implies that A is a bear line. □

Another way to prove the last proposition is using the corollary 7.6 Let $\{p_i\}_{i=0,\dots,q}$ where $p_i = [v_i]$ a subset of H such that is a bear line. This is equivalent to the existence of a line $L = [h(.,v)] \in PG(2,q^2)^*$ such that $L \cap H = \{p_i\}_{i=0,\dots,q}$. This is equivalent to have that $h(v,v_i) = h(v_i,v) = 0$ for all $i = 0,\dots,q$ because $0^q = 0$. This is the same that the tangents of H through p_i are concurrent in $[v]$. Using the corollary 7.6 we have that the tangents of H through p_i are concurrent to $[v]$ if and only if this tangents are a bear line in $PG(2,q^2)^*$.

7.4 Interpreting the results

In this section we will use the above sections in order to understand the results obtained by computer. The first issue is to know why we didn't get an arc.

Proposition 7.8. *Let U be a subspace of $PG(5,q)$ of dimension 3. Let H be a non-degenerate hermitian curve of $PG(2,q^2)$. Then $B(U) \cap H$ isn't an arc.*

Proof. We know that there are two possible cases for $B(U)$ using Proposition 7.2.
Suppose that $B(U)$ is a line. Then $B(U) \cap H$ is a bear line or a point. This implies that it isn't an arc.
Suppose that $B(U)$ is a bear line in $PG(2,q^2)^*$. Suppose that point P is the point where all $q+1$ lines of $B(U)$ are concurrent. If $P \in H$ then at least q lines of $B(U)$ are not tangent to H, since for each point of H there exists a unique tangent. This implies that $B(U) \cap H$ has at least q bear lines. Now suppose $P \notin H$ then we have that the lines that are tangents to H which are concurrent to the same point not in H is a bear line in $PG(2,q^2)^*$. This implies that we have $0, 1, 2, q+1$ lines of $B(U)$ tangent to H. If we have a no tangent line then $B(U) \cap H$ will be an arc. Suppose that all $q+1$ lines of $B(U)$ are tangent to H in points $p_0, \dots, p_q$. This implies that $B(U) \cap H = \{p_0, \dots, p_q\}$. Because of lines contained in $B(U)$ is a bear line in $PG(2,q^2)^*$ and his lines are tangent to p_i, using Proposition 7.7 the points p_i form a bear line. This implies that this case isn't an arc. □

Now we will see the different cases that we can get with the computer for $B(U) \cap H$ where U is a subspace of $PG(5,q)$ of dimension 3 and H is a non-degenerate hermitian curve of $PG(2,q^2)$. To be able to better understand the results it is clear that all lines which intersects in $q+1$ points to $B(U) \cap H$ are bear lines because $H \cap L$ is at most a bear line for any line L.

There are two possible cases for $B(U)$. If $B(U)$ is a line then $B(U) \cap H$ is a bear line or a point. Suppose that $B(U) = \cup_{i=0,\dots,q} L_i$ is a bear line in $PG(2,q^2)$ where $P \in PG(2,q^2)$ is the point that the $q+1$ lines of $B(U)$ are concurrent.
Suppose that $P \in H$ we have two cases: exists L_i such that is tangent to H through P or all L_i are not tangents to H. If exists L_i tangent to H then we have that $L_j \cap H$ is a bear line for $j \neq i$. This implies that $B(U) \cap H$ has at least q bear lines. There are not more bear lines: suppose that exists a bear line that no provide by $L_j \cap H$. This implies that exists a line $L \neq L_j$ for all j such that $L \cap B(U) \cap H$ is a bear line. L has to intersect for each j to $L_j \cap H$ in one different point. But $L_i \cap H = \{P\}$ and $P \in L_j \cap H$ for all j. We get a contradiction because L has to intersect to $L_j \cap H$ to unique different point for each j. This implies that this case has q bear lines. It is easy to see that this case $B(U) \cap H$ has q^2+1 points (Figure 4). Suppose that does not exists any L_j such that is tangent to H. Then we have at least $q+1$ bear lines which are $L_j \cap H$ for each j. This case we have q^2+q+1 points (Figure 5).
Now suppose that $P \notin H$. $B(U)$ and the set of lines which are concurrent to P such that are tangent to H are bear lines in $PG(2,q^2)^*$. For this reason we have that the intersection in $PG(2,q^2)^*$ of this two sets has $0,1,2,q+1$ lines. This implies that $B(U)$ has $0,1,2,q+1$ lines L_j tangents to H. Suppose that we have $q+1$ tangents. Following the proof of the proposition 7.8 we know that this case $B(U) \cap H$ is a bear line (Figure 2). Suppose that we have 2 lines L_i, L_k tangent to H. This case has $q-1$ lines L_j such that $L_j \cap H$ is a bear line. We have to see that this bear lines are all the bear lines of $B(U) \cap H$. Suppose that exists a line $L \neq L_j$ for all j such that $L \cap B(u) \cap H$ is a bear line. Then we have that L has to intersect in only one different point to each $L_j \cap H$. We will call this points p_j. We know that the set $\{p_j\}_{j=0,\dots,q}$ is a bear line. The tangent to H through p_j we will call S_j. Then the set of $PG(2,q^2)^*$ formed by S_j is a bear line. We know that $S_i = L_i, S_k = L_k$ this implies that the point where all line S_j are concurrent is P. This implies that for each S_j share the points P and p_j with L_j. This implies that each $S_j = L_j$. This is a contradiction because we have that some L_j are not tangents. In this case we have $q-1$ bear lines. It is easy to count the points. It has $(q-1)(q+1)+2 = q^2+1$ points. Suppose that we have only L_i such that are tangent to H. This implies that we have q lines L_j such that $L_j \cap H$ is a bear line. This case has at least q bear lines. We can count q^2+q+1 points. The last case is when all L_j are not tangent to H. We have the $q+1$ bear lines $L_j \cap H$. This implies that at least there are $q+1$ bear lines. This case has $(q+1)^2$ points (Figure 3).

The following proposition should help us to count the tangent distribution of $H \cap B(U)$. In the following, U will be a subspace of dimension 3 of $PG(5,q)$ such that there exists only one $P \in PG(2,q^2)$ such that $\psi(P) \subset U$.

Proposition 7.9. *Define a map in the following way: $\varphi : B(U) - \{P\} \longrightarrow U - \psi(P)$ such that $\varphi(Q) = \psi(Q) \cap U$. Then we have that φ defines a bijection between $B(U) - \{P\}$ and $U - \psi(P)$.*

Proof. Firstly we have to check that φ is well defined. Let $Q \in B(U)$ we have that $\psi(Q) \cap U \neq \emptyset$. This implies that $\psi(Q) \cap U$ has dimension 0 or 1. But the only point $Q \in B(U)$ such that $\psi(Q) \cap U$ has dimension 1 is P. This implies that for all $Q \in B(U) - \{P\}$ we have that $\psi(Q) \cap U$ has dimension 0. This implies that it is a point of $U - \psi(P)$ because the images of ψ are disjoint.
Now we will see that φ is surjective. Let S a point of $U - \psi(P)$. We know that $\psi(PG(2,q^2))$ is a partition of $PG(5,q)$. This implies that exists a point $Q \in PG(2,q^2)$ such that $\{S\} \subset \psi(Q)$. We know that $S \in U$

Figure 2: The union of black lines is $B(U)$. The point P is red. The blue points are points of the hermitian curve. The purple line is which contains the bear line. This is a representation for $q = 3$

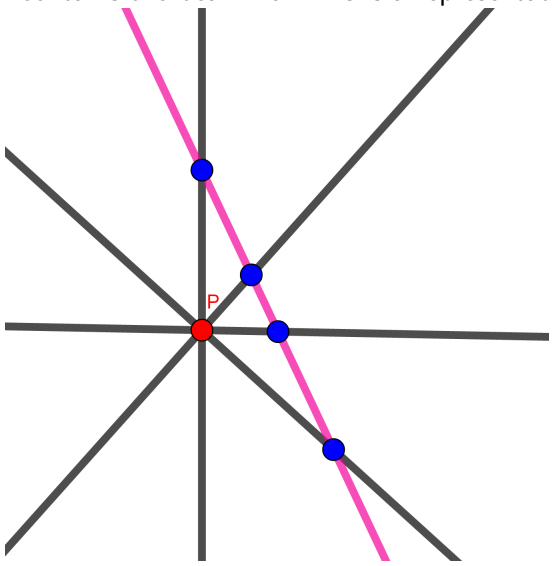
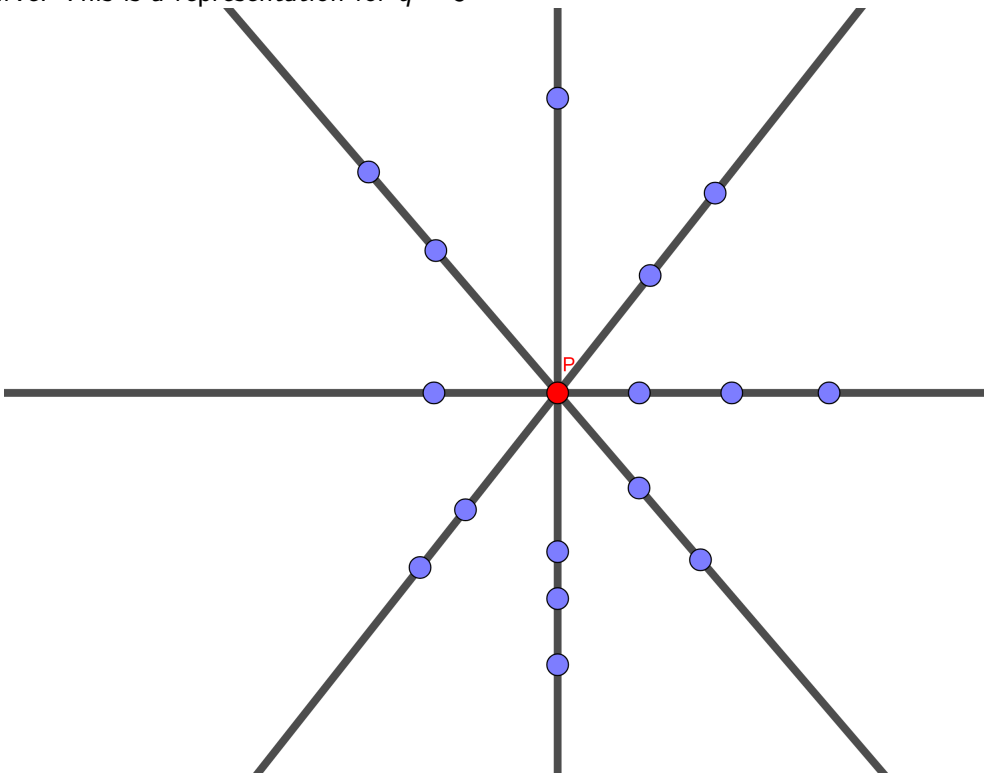


Figure 3: The union of the black lines is $B(U)$. The point P is red. The blue points are points of the hermitian curve. This is a representation for $q = 3$



this implies that $\psi(Q) \cap U \neq \emptyset$. This implies that $Q \in B(U)$ and $Q \neq P$ because $S \notin \psi(P)$. For this reason we have that $\varphi(Q) = S$

Figure 4: The union of the four lines is $B(U)$. The purple line is the tangent line to H. The blue points are in H. This is a representation for $q = 3$

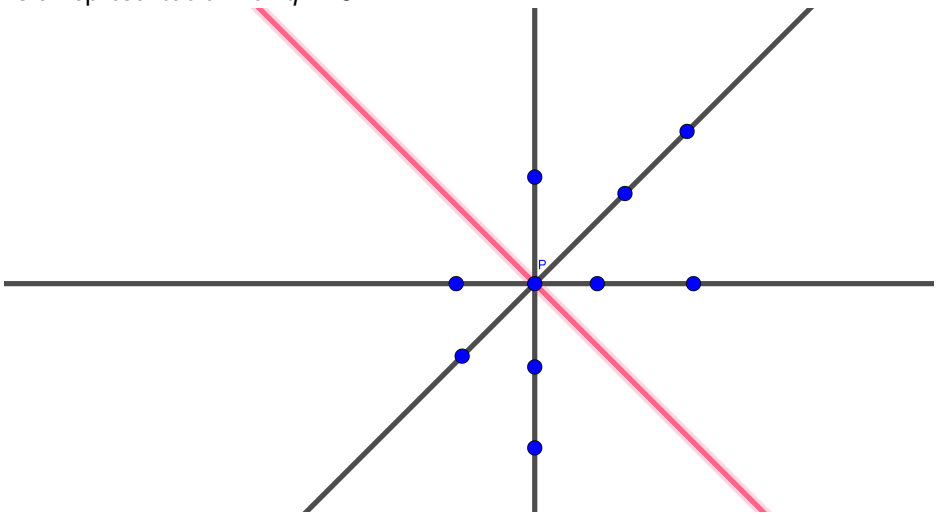
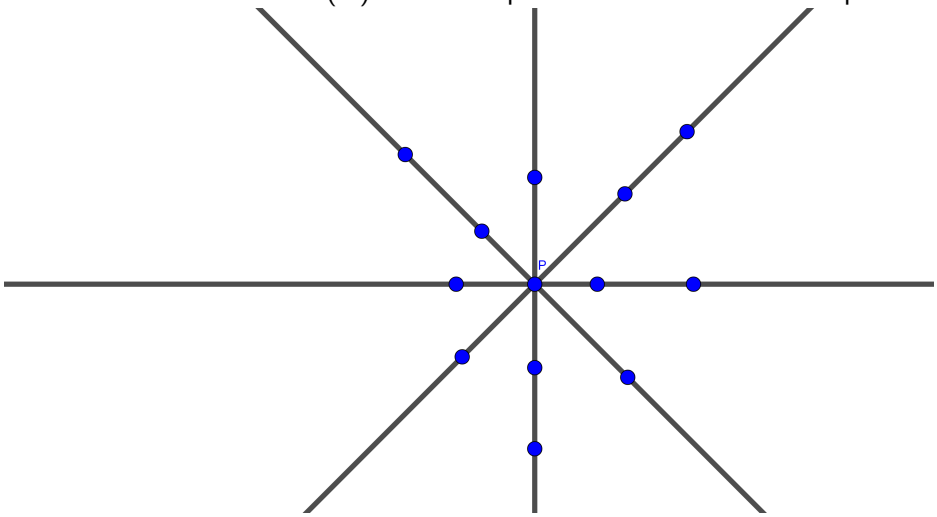


Figure 5: The union of the four lines is $B(U)$. The blue points are in H. This is a representation for $q = 3$



Now we have to check that φ is injective. It is clear because the images of ψ are disjoint. □

Now the objective is define a map between $PG(5,q) \times PG(5,q)$ to $\overline{\mathbb{F}_q} = \mathbb{F}_q \cup \{\infty\}$. This map will help us to identify which lines intersect $B(U) \cap H$ in a bear line. Firstly we observe that for each hermitian form $h : V(3,q^2) \times V(3,q^2) \longrightarrow \mathbb{F}_{q^2}$ can be seen in the following way: $h : V(6,q) \times V(6,q) \longrightarrow \mathbb{F}_{q^2}$, since $V(3,q^2)$ and $V(6,q)$ are isomorphic as vector spaces. Moreover, h is bilinear over $V(6,q)$. Let p, q be two arbitrary points of $PG(5,q)$ represented by $v, u \in V(6,q)$.

Definition 7.10. We define the map $w : PG(5,q) \times PG(5,q) \longrightarrow \overline{\mathbb{F}_q}$. We know that $h(v,u) = c + \epsilon d$ where $c, d \in \mathbb{F}_q$. If $d = 0$ then $w(p,q) = \infty$ else $w(p,q) = \frac{c}{d}$.

We have to check that w is well defined. Suppose that $p = [v_1] = [v_2], q = [u_1] = [u_2] \in PG(2,q^2)$.

This implies that $v_1 = \lambda v_2$ and $u_1 = \mu u_2$. Then we have: $h(v_i, u_i) = c_i + \epsilon d_i$. The following calculation:

$$c_1 + \epsilon d_1 = h(v_1, u_1) = \lambda\mu h(v_2, u_2) = \lambda\mu(c_2 + \epsilon d_2) = \lambda\mu c_2 + \epsilon\lambda\mu d_2$$

implies $c_1 = \lambda\mu c_2$ and $d_1 = \lambda\mu d_2$. Then we have that $d_1 = 0$ if and only if $d_2 = 0$ or $\frac{c_1}{d_1} = \frac{c_2}{d_2}$. This tells us that w not does not depend on the representation of the points.

The following proposition gived information about the intersection between $B(U) \cap H$ and lines L such that $\psi(L) \cap U$ has dimension 1. In this proposition we have to suppose that q is odd because we will need that the field doesn't have characteristic 2.

Proposition 7.11. *Suppose that q is odd. Let H be a non-degenerate hermitian curve of $PG(2, q^2)$ represented by h. Let $p, q \in PG(2, q^2)$ and L the line defined by p, q. Suppose $\psi(L) \cap U$ has dimension 1. Then we have two cases:*

- *If $w(\varphi(p), \varphi(q)) \neq -\frac{a}{2}$ then we have that $B(U) \cap H \cap L = \{p, q\}$.*
- *If $w(\varphi(p), \varphi(q)) = -\frac{a}{2}$ then we have that $B(U) \cap H \cap L$ is a bear line.*

Proof. In this situation we know that $V(6, q)$ is the same set as $V(3, q^2)$ only change the structure of linear space. For this reason for each $v \in V(3, q^2)$ we will denote $[v]_{\mathbb{F}_{q^2}} \in PG(2, q^2)$ or $[v]_{\mathbb{F}_q} \in PG(5, q)$. Suppose that $\varphi(p) = [u]_{\mathbb{F}_q}, \varphi(q) = [v]_{\mathbb{F}_q} \in PG(5, q)$. We want to know which points of L are in $B(U) \cap H$. In the basis u, v of L all points have the form $[(x_1 + \epsilon x_2, 1)]$ where $x_1, x_2 \in \mathbb{F}_q$ or $[(1, 0)]$. We know that $[(1, 0)]$ is in $B(U) \cap H$. The objective is to find equations that relate the variables x_1, x_2 imposing the condition that $[(x_1 + \epsilon x_2, 1)]$ has to be in $B(U) \cap H$.

Since $\psi(L) \cap U$ has dimension 1 and $p, q \in B(U)$ we have that $\psi(L) \cap U =< u, v >$. A point $Q \in L$ is in $B(U)$ if and only if $< \psi(Q), u, v >$ has rank at most 3. To calculate $\psi|_L$ we take the basis $u, v, \epsilon u, \epsilon v$ in $\psi(L)$. We can calculate $\psi(Q) =< (x_1, 1, x_2, 0), (bx_2, 0, x_1 + ax_2, 1) >$ in the same way as Subsection 7.1.

$$\begin{vmatrix} x_1 & bx_2 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ x_2 & x_1 + ax_2 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix} = 0 \Leftrightarrow x_2 = 0 \tag{8}$$

It's important to remember that $\epsilon, \bar{\epsilon}$ are zeros of the polynomial $x^2 - ax - b$. Now the objective is to find an equation for the points of L in H of the form $[(x_1 + \epsilon x_2, 1)]$ in the basis v, u. Since $[u]_{\mathbb{F}_q} \subset [u]_{\mathbb{F}_{q^2}} = p \in H$ and $[v]_{\mathbb{F}_q} \subset [v]_{\mathbb{F}_{q^2}} = q \in H$ we have that $h(u, u) = h(v, v) = 0$ and $h(u, v) \neq 0$. Rearranging u, v in $\mathbb{F}_q$ so that the relations $[u]_{\mathbb{F}_q} = \varphi(p)$ and $[v]_{\mathbb{F}_q} = \varphi(q)$ continue to be true we can suppose that $h(u, v) = c + \epsilon$ or $h(u, v) = 1$ where $c \in \mathbb{F}_q$.
Suppose that $w(\varphi(p), \varphi(q)) = \infty \neq -\frac{a}{2}$. This implies that we have $h(u, v) = 1$. Then we have the following equation:

$$0 = (x_1 + \epsilon x_2)^q + (x_1 + \epsilon x_2) = 2x_1 + ax_2 = 0 \tag{9}$$

Using the equation of $B(U)$ and the H we have that the only points of L in $B(U) \cap H$ are $[(1, 0)] = p$ and $[(0, 1)] = q$. Suppose that $w(\varphi(p), \varphi(q)) \neq \infty$, this implies that $h(u, v) = c + \epsilon$ where $c = w(\varphi(p), \varphi(q)) \in \mathbb{F}_q$. Now we have the following equation:

$$0 = (x_1 + \epsilon x_2)h(u, v) + (x_1 + \epsilon x_2)^q h(v, u) = (x_1 + \epsilon x_2)(c + \epsilon) + (x_1 + \epsilon x_2)(c + \epsilon)^q \Leftrightarrow$$

$$(2c + a)x_1 + (...)x_2 = 0 \tag{10}$$

Using the equation of $B(U)$ and the H we have the following system:

$$\begin{cases} (2c+a)x_1 + (...)x_2 = 0 \\ x_2 = 0 \end{cases} \Leftrightarrow \begin{cases} (2c+a)x_1 = 0 \\ x_2 = 0 \end{cases}$$

If we have $c \neq -\frac{a}{2}$ then all points of L in $B(U) \cap H$ are $[(1,0)] = p$ and $[(0,1)] = q$. Suppose that $c = -\frac{a}{2}$. This implies that $L \cap B(U) \cap H = \{[(x_1, 1)]\}_{x_1 \in \mathbb{F}_q} \cup \{[(1,0)]\}$, which is a bear line. □

We will see what happen if the characteristic of the field is two. In terms of counting it happen the same as in odd characteristic.

Proposition 7.12. *Suppose that q is even. Let H be a non-degenerate hermitian curve of $PG(2, q^2)$ represented by h. Let $p, q \in PG(2, q^2)$ and L the line defined by p, q. Suppose $\psi(L) \cap U$ has dimension 1. Then we have two cases:*

- *If $w(\varphi(p), \varphi(q)) \neq \infty$ then we have that $B(U) \cap H \cap L = \{p, q\}$.*
- *If $w(\varphi(p), \varphi(q)) = \infty$ then we have that $B(U) \cap H \cap L$ is a bear line.*

Proof. We can do the same procedure as the proposition 7.11 to obtain the equations. Suppose that $w(\varphi(p), \varphi(q)) = \infty$. This implies that $h(u, v) = 1$. The equations (8), (9) in characteristic 2 are equivalent to $x_2 = 0$. This implies that we have the bear line $[(x_1, 1)]$ where $x_1 \in \mathbb{F}_q$ and $[(1,0)]$. Suppose that $h(u, v) = c + \epsilon$. Using the equations (8), (10) where the points have the expression $[(x_1 + \epsilon x_2, 1)]$ on the basis u, v we get the following system:

$$\begin{cases} (2c+a)x_1 = 0 \\ x_2 = 0 \end{cases} \Leftrightarrow \begin{cases} x_1 = 0 \\ x_2 = 0 \end{cases}$$

We can do the last step because the characteristic of the field is 2. We have to check that $a \neq 0$. We know that $x^2 - ax - b$ is a irreducible polynomial in $\mathbb{F}_q$. If $a = 0$ then the polynomial has the form $x^2 - b$. Because of the morphism $x \to x^2$ is exhaustive in $\mathbb{F}_q$ take $d^2 = b$ where $d \in \mathbb{F}_q$. This implies that $(x - d)^2 = x^2 - b$. This is a contradiction because $x^2 - b$ is irreducible. It says us that $a \neq 0$.
Seeing the system of equations we will see that $L \cap B(U) \cap H$ has only the points p, q in this case. □

Now U can be any subspace of $PG(5, q)$. We will prove that if U is not scattered then $B(U) \cap H$ can not be an arc. This says us that we can construct and arc with the form $B(U) \cap H$ using spaces of dimension bigger than 2.

Proposition 7.13. *Let H be a non-degenerate hermitian curve of $PG(2, q^2)$. Let U be a subspace of $PG(5, q)$. If $B(U) \cap H$ is an arc then U is scattered.*

Proof. We will prove that if U is not scattered then $B(U) \cap H$ is not an arc. Suppose that U has dimension at least 3. Take a subspace V of U of dimension 3. Then using the proposition 7.8 we have that $B(V) \cap H$ is not an arc. It is clear that $B(V) \cap H \subset B(U) \cap H$ because $U \subset V$. This implies that $B(U) \cap H$ is not an arc. Suppose that U has dimension 2. We know that exists $P \in PG(2, q^2)$ such that $\psi(P) \subset U$. This implies that $U =< u, \epsilon u, v >$ where $P = [v]$. We want to see that $B(U) \subset L$ where L is the line defined by P and $[v]$. It is clear that every linear combination of $u, \epsilon u, v$ corresponds to a point in L. Then this implies that $B(U) \cap H$ is contained in a line and an arc never will lie in a line because it has to have more than 3 points. If U has dimension 1 a it is not scattered $B(U)$ will be a point. If U is not scattered then U can not have dimension 0. □

If we want that $B(U) \cap H$ will be an arc we have to impose that U will be an scattered space. Because of the proposition 6.9 the dimension of U has to be at most 2 and exists scattered spaces of this dimension. There is a bijection between U and $B(U)$. We can see the set H in U as a conic. This implies that set $B(U) \cap H$ will have the same number of points of $H \cap U$ and it will be $q+1$. If we get a U such that $B(U) \cap H$ is an arc then it will be a small arc of $PG(2, q^2)$.

Now we will develop a method to construct an arc using a scattered subspace U of $PG(5, q)$. In the following enunciates U will be a scattered subspace of $PG(5, q)$ but in practice it will be of dimension 2.

Lemma 7.14. *Let L be a line of $PG(2, q^2)$ such that $\psi(L) \cap U$ has dimension at least 2. Then exists $P \in L$ such that $\psi(P) \subset U$.*

Proof. If $\psi(L) \cap U$ has at least dimension 3 then $\psi(L) \subset U$ and the proof follows. Suppose that $\psi(L) \cap U$ has dimension 2. This implies that $\psi(L) \cap U$ has q^2+q+1 points. For each point $Q \in L$ we have that $\psi(Q) \cap U$ has 1 or $q+1$ points. Because of the line has q^2+1 points the only possibility is that there are only one point such that $\psi(Q) \cap U$ has $q+1$ points. This implies that this point has the property that $\psi(Q) \subset U$ because $\psi(Q)$ is a line and has $q+1$ points. □

Note that for each line L of $PG(2, q^2)$ $\psi(L) \cap U$ can have dimension $-1, 0, 1$. If it has dimension -1 then $L \cap B(U) = \emptyset$. If it has dimension 0 then $L \cap B(U)$ has only one point. If it has dimension 1 using the proposition 5.10 we get that $L \cap B(U)$ is a bear line. We will use this in the following theorem that prove the existence of an arc with the form $B(U) \cap H$.

Theorem 7.15. *Let H be a non-degenerate hermitian curve of $PG(2, q^2)$ such that seen as a quadratic form in U will be non-degenerate. Suppose that U has dimension 2. Then $B(U) \cap H$ is an arc of $q+1$ points.*

Proof. Let L be a line of $PG(2, q^2)$. Suppose that L intersects with $B(U) \cap H$ in at least 3 points. Then implies that $L \cap B(U)$ is a bear line. Because of U is scattered there are a bijection between the points of the bear line $L \cap B(U)$ and the line $S = \psi(L) \cap U$. This implies that that the line S is contained in the quadric of U defined by H. It is a contradiction because the intersection between a non-degenerate quadric and a line has at most two points. This implies that $L \cap B(U) \cap H$ has at most two points.
It is clear that $B(U) \cap H$ has $q+1$ points because the quadric H in U has $q+1$ points. □

Using the last theorem and the proposition 6.9 for the existence of a scattered space of dimension 2 we can construct an arc with the form $B(U) \cap H$.

8. Bibliography

References

[1] S. Ball, *Finite Geometry and Combinatorial Applications*, London Mathematical Society Student Texts **82**, Cambridge University Press, 2015.

[2] S. Ball and Zs. Weiner, *An introduction to Finite Geometry*,

`https://mat-web.upc.edu/people/simeon.michael.ball/IFG.pdf`

[3] B. C. Kestenband, Unital intersections in finite projective planes, *Geom. Dedicata*, **11** (1981) 107–117.

[4] , M. Lavrauw, *Scattered Spaces with respect to Spreads, and Eggs in Finite Projective Spaces*, Ph. D Thesis, Technische Universiteit Eindhoven, 2001.

[5] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.*, **7** (1955) 414-416.

A. Codes of GAP

A.1 Calculus of function sigma

```
SigmaF:=function(v,q)
local x,y,z,e,x1,x2,y1,y2,z1,z2,a,b,p,s,i,L,t;
e:= Z(q^2);;
t:= Indeterminate(GF(q^2),"t");;
p:= (t-e)*(t-e^q);;
L:= CoefficientsOfUnivariatePolynomial(p);;
b:= -L[1];; a:= -L[2];;
x:= v[1];; y:= v[2];; z:= v[3];;
i:= PositionSorted(SET,x);
x1:= Coords[i][3];;
x2:= Coords[i][2];;
i:= PositionSorted(SET,y);
y1:= Coords[i][3];;
y2:= Coords[i][2];;
i:= PositionSorted(SET,z);
z1:= Coords[i][3];;
z2:= Coords[i][2];;
return [[x1,y1,z1,x2,y2,z2],[x2*b,y2*b,z2*b,x1+x2*a,y1+y2*a,z1+z2*a]];
end;
```

This function return $\psi(P)$. For to factorize a number $x \in \mathbb{F}_{q^2}$ to the form $x_1 + \epsilon x_2$ use a sorted table that there are all the numbers of $\mathbb{F}_{q^2}$ factorized. This table is named coords.

A.2 Construction of random linear set

```
Burbuja:=function(q)
local B,s,v1,v2,v3,v4,u,p,x,y,M,R,o,S5;
s:= RootInt(q);

B:=[];;

v1:= [One(GF(s)),Zero(GF(s)),Zero(GF(s)),Zero(GF(s)),Random(GF(s)),Random(GF(s))];;
v2:= [Zero(GF(s)),One(GF(s)),Zero(GF(s)),Zero(GF(s)),Random(GF(s)),Random(GF(s))];;
v3:= [Zero(GF(s)),Zero(GF(s)),One(GF(s)),Zero(GF(s)),Random(GF(s)),Random(GF(s))];;
v4:= [Zero(GF(s)),Zero(GF(s)),Zero(GF(s)),One(GF(s)),Random(GF(s)),Random(GF(s))];;

S5:= Group([(1,2),(1,2,3,4,5,6)]);;
o:= Random(S5);;

u:= ShallowCopy(v1);;
for i in [1..6] do
```

```
v1[i^o]:= u[i];;
od;

u:= ShallowCopy(v2);;
for i in [1..6] do
v2[i^o]:= u[i];;
od;

u:= ShallowCopy(v3);;
for i in [1..6] do
v3[i^o]:= u[i];;
od;

u:= ShallowCopy(v4);;
for i in [1..6] do
v4[i^o]:= u[i];;
od;

M:= [v1,v2,v3,v4];;
for x in GF(q) do
for y in GF(q) do
p:= [One(GF(q)),x,y];;
R:= SigmaF(p,s);;
M[5]:= R[1];;
M[6]:= R[2];;
if RankMat(M) < 6 then
AddSet(B,p);
fi;
od;
od;

for y in GF(q) do
p:= [Zero(GF(q)),One(GF(q)),y];;
R:= SigmaF(p,s);;
M[5]:= R[1];;
M[6]:= R[2];;
if RankMat(M) < 6 then
AddSet(B,p);
fi;
od;

p:= [Zero(GF(q)),Zero(GF(q)),One(GF(q))];;
R:= SigmaF(p,s);;
M[5]:= R[1];;
M[6]:= R[2];;
if RankMat(M) < 6 then
```

```
AddSet(B,p);
fi;
return B;
end;
```

Firstly we choose a random vector subspace U of rank 4. Then for all points of $PG(2, q^2)$ we check if $\psi(P) + U$ has rank at most 5.

A.3 Hermitian curve

```
HermitianCurve:=function(q)

local S,H, s,i,j,x1,x2;

s:=RootInt(q);

H:=[[0,1,0],[1,0,0],[0,0,1]];
H:= One(GF(q))*H;


S:=[];
for x1 in GF(q) do
for x2 in GF(q) do
if [Z(q)^0,x1,x2]*H*[Z(q)^0,x1^s,x2^s]=0*Z(q) then
AddSet(S,[Z(q)^0,x1,x2]);
fi;
od;
od;

for x1 in GF(q) do
if [Z(q)*0,Z(q)^0,x1]*H*[Z(q)*0,Z(q)^0,x1^s]=0*Z(q) then
AddSet(S,[Z(q)*0,Z(q)^0,x1]);
fi;
od;

if [Z(q)*0,Z(q)*0,Z(q)^0]*H*[Z(q)*0,Z(q)*0,Z(q)^0]=0*Z(q) then
AddSet(S,[Z(q)*0,Z(q)*0,Z(q)^0]);
fi;

return S;
end;
```

This function return the set of points of the hermitian curve $xy^q + yx^q + z^{q+1} = 0$. This function calculate it for each point if $PG(2, q^2)$ is in H.

A.4 Secant distribution

```
SecantDistribution:=function(S,q)

local x1,x2,j,tau,a,sec;

tau:=[];
for j in [1..(q+1)] do
tau[j]:=0;
od;
for x1 in GF(q) do
for x2 in GF(q) do
sec:=0;
for a in [1..Size(S)] do
if (x1*S[a][1]+x2*S[a][2]+Z(q)^0*S[a][3])=0*Z(q) then
sec:=sec+1;
fi;
od;
if sec<>0 then
tau[sec]:=tau[sec]+1;
fi;
od;
od;
for x1 in GF(q) do
sec:=0;
for a in [1..Size(S)] do
if x1*S[a][1]+Z(q)^0*S[a][2]=0*Z(q) then
sec:=sec+1;
fi;
od;
if sec<>0 then
tau[sec]:=tau[sec]+1;
fi;
od;
sec:=0;
for a in [1..Size(S)] do
if S[a][1]=0*Z(q) then
sec:=sec+1;
fi;
od;
if sec<>0 then
tau[sec]:=tau[sec]+1;
fi;

return(tau);
end;
```

This function returns a vector with the secant distribution of the set S. It calculate the secant distribution counting the points that each line intersects with S.

A.5 Intersection between H and $B(U)$

```
q = 11^2;
s = RootInt(q);
SET:= Set(GF(q));;
#taula per escriure els numeros en funció del del cos petit.
Coords:=[];;
for i in GF(s) do
for j in GF(s) do
AddSet(Coords,[i*Z(q)+j,i,j]);;
od;
od;
U:=HermitianCurve(q);;
for b in [1..100] do
T:=Burbuja(q);
S:=Intersection(T,U);;
tau:=SecantDistribution(S,q);;
Print(Size(S)," ",tau," ","\n");
od;
```

This is the main code. It calculates the intersection between a H and $B(U)$. It calculate the table coords that is vector of vectors (x, x_1, x_2). It is useful to calculate the factorization very fast.